Lenovo XClarity Administrator
Guia de Determinação de Problema

Versão 4.3

Nota

Antes de usar estas informações e o produto ao qual elas dão suporte, leia os avisos gerais e legais do na documentação online do XClarity Administrator.

Quarta edição (Abril 2025)

© Copyright Lenovo 2015, 2025.
AVISO DE DIREITOS LIMITADOS E RESTRITOS: se dados ou software forem fornecidos de acordo com um contrato de Administração de Serviços Geral, ou "GSA", o uso, a reprodução ou a divulgação estarão sujeitos às restrições definidas no Contrato No. GS-35F-05925.

Conteúdo

Conteúdo i

Resumo de alterações v

Capítulo 1. Obtendo ajuda e assistência técnica 1

Capítulo 2. Exibindo alertas, eventos e trabalhos 3

Colocando dispositivos no modo de manutenção . . 3
Trabalhando com alertas 4
Visualizando alertas ativos 4
Excluindo alertas 8
Resolvendo um alerta. 9
Confirmando alertas 10
Trabalhando com eventos. 10
Monitorando eventos no log de eventos . . . 11
Monitorando eventos no log de auditoria . . . 13
Resolvendo um evento 14
Excluindo eventos 15
Encaminhamento de eventos. 16
Trabalhando com trabalhos 50
Monitorando trabalhos 51
Programando trabalhos 53
Adicionando uma resolução e comentários a um trabalho 56

Capítulo 3. Trabalhando com serviço e suporte 57

Obtendo boletins da Lenovo 57
Visualizando informações sobre garantia 58
Configurando uma notificação de problema automática. 59
Configurando a notificação automática do problema para o Suporte Lenovo (Call Home). 60
Configurando a notificação automática de problema para o Recurso de Upload da Lenovo 66
Configurando a notificação de problema automática em um provedor de serviços preferencial 70
Alterando a senha de recuperação de serviço . . . 73
Inspecionando arquivos de serviço 73
Definindo os contatos de suporte para dispositivos específicos 74
Coletando e baixando dados de serviço de um dispositivo 74
Coletando e baixando arquivos de serviço do Lenovo XClarity Administrator 76
Coletando e baixando arquivos de serviço para um Lenovo XClarity Administrator que não responde 78
Enviando uma solicitação de serviço para problemas de hardware para o Centro de Suporte da Lenovo 79
Relatando problemas do XClarity Administrator . . 81
Anexando um arquivo de serviço a um tíquete de serviço aberto 83
Exibindo tíquetes de serviço e o status. 84
Transferindo arquivos de serviço para o Suporte Lenovo 85
Definindo configurações de log do servidor de gerenciamento 86
Reativando Call Home em todos os dispositivos gerenciados 87
Enviando dados periódicos à Lenovo 87
Dados de uso de amostra 89
Dados de hardware de amostra. 92

Capítulo 4. Gerenciando espaço em disco 109

Capítulo 5. Problemas de descoberta e gerenciamento 113

Não é possível descobrir um dispositivo 113
Não é possível gerenciar um dispositivo 114
Não é possível gerenciar um dispositivo de armazenamento devido a um certificado SSL/TSL inválido 117
Não é possível gerenciar um comutador devido a um certificado SSL/TSL inválido 117
Não é possível recuperar a conectividade de um chassi do Flex System gerenciado após a substituição da placa de LED traseira ou do conjunto do painel intermediário 117
Não é possível recuperar a conectividade de um servidor gerenciado depois de substituir a placa-mãe 118
O encapsulamento não foi desativado depois do cancelamento do gerenciamento de um servidor 118
Nó de cálculo não é exibido na interface do usuário depois do gerenciamento. 119
O estado de energia do servidor está incorreto . . 119

Capítulo 6. Problemas de instalação, remoção, atualização e migração de dados. 121

© Copyright Lenovo 2015, 2025

A saída de vídeo não é exibida ao instalar o XClarity Administrator em Red Hat KVM 121
As alterações de adaptador não são reconhecidas 121
Durante a configuração inicial, não é possível abrir o assistente de configuração Inicial em um navegador da Web 121
Falha inesperada de implantação do Lenovo XClarity Administrator 121
Falha na atualização do Lenovo XClarity Administrator 122

Capítulo 7. Problemas de conectividade 123
Não é possível acessar o Lenovo XClarity Administrator 123
Não é possível estabelecer uma conexão com o Lenovo XClarity Administrator usando o navegador Safari 123
Não é possível efetuar login 123
Não é possível fazer login no Lenovo XClarity Administrator 123
A senha de um usuário supervisor ou de recuperação local foi esquecida 124
Não é possível fazer login no CMM gerenciado diretamente 127
Não é possível fazer login diretamente no controlador de gerenciamento 127
Não é possível acessar servidores gerenciados do Flex Power System 127
Perda repentina de conectividade com um dispositivo 128

Capítulo 8. Problemas de configuração do Lenovo XClarity Administrator 129
Problemas de configuração de LDAP externo . . . 129
O usuário não possui autorização suficiente para configurar servidores 129
Problemas de ativação do Features on Demand 129
VMware avisa que o driver VMXNET 3 não é suportado 129

Capítulo 9. Problemas de desempenho 131
Problemas de desempenho do Lenovo XClarity Administrator 131
Desempenho de rede insatisfatório ou lento 131

Capítulo 10. Problemas de segurança 133
Não é possível confiar no certificado SSL 133
Falha na validação de certificação do servidor . . . 133
Vulnerabilidades do Samba e do Apache 134

Capítulo 11. Solução de problemas de backup e restauração 137
O processo de backup parece ter sido interrompido durante a reinicialização do servidor de gerenciamento 137
A janela do XClarity Administrator fica em branco após a atualização durante o backup 137

Capítulo 12. Problemas de monitoramento e transmissão de evento 139
Os eventos não são encaminhados 139

Capítulo 13. Problemas de gerenciamento de dispositivos 141
Não é possível apagar com segurança os dados em unidades paralisadas 141
Não é possível apagar com segurança volumes SDD SATA quando conectados ao Marvel RAID 141
Os dados do inventário não são atualizados depois de adicionar ou substituir placas 141

Capítulo 14. Problemas de configuração do servidor 143
Ocorre um erro ao criar um padrão de um servidor existente 143
Ao implantar um padrão em um dispositivo, ocorre um erro de ativação 143
Uma configuração inválida foi implantada em um comutador 144

Capítulo 15. Problemas de repositório e atualização de firmware 145
Falha ao conectar-se ao repositório Lenovo 145
Após a atualização de firmware, a página Aplicar/Ativar não mostra versões do firmware atualizadas 145
Não é possível atualizar o firmware em um dispositivo 145
A atualização de firmware do CMM trava 145
O firmware está atualizado, mas não realiza a verificação de conformidade 146
Atualizações de firmware em comutadores Flex System falham inesperadamente 146
A atualização de firmware no comutador Flex falhou, indicando um erro com a mensagem "Falha na operação de download de firmware." 147
A atualização de firmware no comutador Flex falhou, indicando um erro com a mensagem "DCSS_RC_CDT_FAIL" 147
A atualização de firmware no comutador Flex falhou, indicando um erro com a mensagem de "tempo limite" 147

A atualização de firmware no comutador Flex falhou, indicando um erro com a mensagem "Não é possível baixar a mesma versão do firmware. Baixe outro firmware." 147
A atualização de firmware no comutador Flex falhou, indicando um erro com a mensagem de falha ao contatar o host. 148
A atualização de firmware no comutador Flex falhou, indicando um erro com a mensagem "o arquivo não existe" 148
A atualização de firmware no comutador Flex falhou, indicando um erro com a mensagem "falha quando a luz para de piscar" 148
Falha inesperada na atualização de firmware no Comutador Ethernet de 40 Gb EN6131 ou no Comutador InfiniBand IB6131 148
Falha na atualização de firmware no módulo intermediário Lenovo EN4091 149
A atualização de firmware no comutador Flex System falhou, indicando um erro com a mensagem "Falha de autenticação da chave do host" 149
Ao executar uma atualização, o sistema não entra no modo de manutenção 149
Reiniciar um servidor do sistema operacional não ativa o modo de manutenção 150
O servidor executando o Red Hat Enterprise Linux (RHEL) não reinicia 150

Capítulo 16. Problemas de repositório e atualização de driver de dispositivo do SO 151

Não é possível se conectar ao site de suporte da Lenovo para baixar atualizações de drivers de dispositivo 151
Não é possível atualizar drivers de dispositivo em um servidor 151

Capítulo 17. Problemas de implantação do sistema operacional 153

Problemas no relatório de status durante a implantação do SO 153
Não é possível implantar um sistema operacional 153
Não é possível importar um arquivo para o repositório de imagens do SO 154
O instalador do SO não pode localizar a unidade de disco em que você deseja instalar 155
O instalador do SO não pode inicializar em um servidor ThinkServer 155
Problemas de implantação do VMware ESXi . . . 156
A implantação do VMware trava ou reinicia o sistema 156
Falha de implantação do VMware com erros de disco 156
O sistema operacional não é reinicializado para concluir a implantação do ESXi em um servidor ThinkServer 157
Problemas de implantação do Red Hat e do SUSE Linux 157
O Redhat 6.x não pode ser implantado em servidor baseado em rack com IP estático . . 158
Falha na implantação do SO devido a drivers ausentes 158
Problemas de implantação do Microsoft Windows 158
A implementação do SO falha devido a partições do sistema existentes em uma unidade de disco conectada 158

Capítulo 18. Problemas de controle remoto 161

A sessão de controle remoto não inicia. 161
A sessão de controle remoto trava após o login . . 161
Não é possível conectar-se a um servidor 162
Não é possível se comunicar com um comutador Flex System após iniciar uma sessão de controle remoto 162
Não é possível conectar-se a um servidor no modo de usuário único 162
O Controle Remoto pode se conectar a um servidor, mas nenhum vídeo está disponível. . . . 163
Um servidor não aparece na lista para incluir uma nova sessão 163
O estado do servidor na sessão de controle remoto não corresponde ao estado no Lenovo XClarity Administrator 163
Uma unidade ou imagem não pode ser montada em um servidor 164
A opção de mídia de armazenamento não é mostrada na lista de dispositivos de mídia remota disponíveis para montagem 164
A operação de energia não pode ser executada 164
Vídeo indisponível ao conectar no Servidores Flex System x280 X6, x480 X6 e x880 X6 165

Capítulo 19. Problemas da interface do usuário 167

Itens de menu, ícones da barra de ferramentas e botões estão desativados (esmaecidos) 167
Navegador da Web não responde quando várias guias estão abertas 167
Falha na resposta de JSON, erro de análise e outros erros inesperados 167
A interface do usuário não está no idioma preferencial 167
Tempos de carregamento lentos ou aparentemente sem resposta, longa espera para atualizar, renderização incorreta 168
Perda de dados inesperada 168

© Copyright Lenovo 2015, 2025

As alterações de local do dispositivo não são refletidas na exibição de rack 168

Resumo de alterações

Versões de acompanhamento do software de gerenciamento Lenovo XClarity Administrator oferecem suporte aos novos aprimoramentos de hardware, software e correções.

Consulte o arquivo de histórico de alterações (*.chg) fornecido no pacote de atualizações para obter informações sobre as correções.

Não há aprimoramentos para determinação e resolução de problemas nesta versão.

Esta versão oferece suporte aos seguintes aprimoramentos para determinação e resolução de problemas.

Para obter informações sobre alterações nas versões anteriores, consulte O que há de novo na documentação online do XClarity Administrator.

Função	Descrição
Serviço e Suporte	O suporte para a API tcpdump foi adicionado para ajudar o Suporte Lenovo durante as interações com o cliente.

© Copyright Lenovo 2015, 2025

Capítulo 1. Obtendo ajuda e assistência técnica

Se precisar de ajuda, serviços ou assistência técnica para Lenovo XClarity Administrator, você poderá encontrar uma ampla variedade de fontes de informação que a Lenovo disponibiliza para ajudá-lo.

Antes de iniciar

Para obter informações gerais sobre números de contato, recursos e diretrizes para ajudá-lo a obter o melhor suporte possível quando e onde você precisar, consulte o Plano de suporte Lenovo – Página da Web de software.

Procedimento

- Faça perguntas e encontre respostas clicando no menu de ações do usuário (

) na barra de título XClarity Administrator e, em seguida, clicando em **Visitar fórum** ou indo diretamente para o Site do fórum da comunidade do Lenovo XClarity.
- Envie ideias sobre o XClarity Administrator clicando no menu de ações do usuário (

) na barra de título XClarity Administrator e, em seguida, clicando em **Enviar ideias** ou indo diretamente para o Web site de concepção do Lenovo XClarity.
- Verifique o log de eventos e siga as ações sugeridas para resolver os códigos de eventos (consulte Trabalhando com eventos).
- Encontre soluções para problemas que possuem sintomas identificáveis e siga as ações sugeridas para resolver quaisquer problemas. Para ver os procedimentos mais recentes de solução de problemas, consulte Solução de problemas na documentação online do XClarity Administrator.
- Confira o Site de Suporte a data center da Lenovo para obter dicas e técnicas mais recentes que você pode usar para resolver problemas que podem acontecer com o XClarity Administrator. Essas *dicas técnicas* fornecem procedimentos para solucionar problemas relacionados ao funcionamento do XClarity Administrator.

  Para localizar as dicas técnicas disponíveis para seu servidor:

  1. Acesse Site de Suporte a data center da Lenovo.
  2. Insira "XClarity Administrator" no campo **Pesquisar**.
  3. Clique em **Exibir Tudo** na seção **Principais Artigos** para exibir todas as dicas ou insira palavras-chave no campo **Pesquisar** para obter uma dica específica.

     Dica: É possível classificar a lista pelas dicas **Relevância**, **Popularidade** ou **Mais novo**.
- Se o problema for um problema de hardware ou de Baseboard Management Controller com um dispositivo gerenciado, consulte a documentação fornecida com o dispositivo para obter informações sobre problemas e ações sugeridas.
  - Para dispositivos ThinkAgile, consulte o Documentação online do ThinkAgile.
  - Para produtos ThinkSystem, incluindo servidores e dispositivos de rede, consulte o Documentação online do ThinkSystem.
  - Para produtos Converged, System x e RackSwitch, incluindo servidores e comutadores top-of-rack, consulte Documentação online do System x.
  - Para produtos NeXtScale, consulte Documentação online do NeXtScale.
  - Para produtos Flex System, incluindo chassis, comutadores, dispositivos de armazenamento e nós de cálculo, consulte Documentação online do Lenovo Flex System.

© Copyright Lenovo 2015, 2025

- Se o problema for com o servidor de gerenciamento XClarity Administrator, é possível enviar manualmente um tíquete de serviço (consulte Relatando problemas do XClarity Administrator).
- Se o problema persistir, e você for um cliente com um contrato de linha de suporte, contratos de manutenção de e/ou garantia, envie uma solicitação de serviço online.

  Nota: O Lenovo XClarity Pro fornece direito ao serviço e suporte e a licença de habilitação com funcionalidade completa para o XClarity Administrator. Para obter informações sobre a aquisição do Lenovo XClarity Pro, entre em contato com seu representante Lenovo ou o parceiro de negócios autorizado.

  Enviar uma solicitação de serviço inicia o processo para determinar uma solução para seu problema disponibilizando as informações pertinentes para o Suporte da Lenovo de maneira rápida e eficiente. Os técnicos de serviço do Lenovo poderão começar a trabalhar em sua solução assim que você tiver concluído e enviado uma solicitação.

  Nota: Se um Call Home está configurado e habilitado, o XClarity Administrator abre automaticamente um tíquete de serviço e transfere os arquivos de serviço para o Centro de Suporte da Lenovo quando ocorre um evento que permite manutenção em um dispositivo gerenciado para que o problema possa ser resolvido. Para obter informações sobre como ativar o Call Home, consulte Configurando a notificação automática do problema para o Suporte Lenovo (Call Home).

  Se o Call Home não estiver habilitado, será possível enviar manualmente uma solicitação de serviço e enviar arquivos de serviço (consulte Enviando uma solicitação de serviço para problemas de hardware para o Centro de Suporte da Lenovo).

  Nota: A IBM é o provedor de serviço preferencial do Lenovo para XClarity Administrator. As solicitações de serviço para alguns dispositivos são encaminhadas para a IBM para obter assistência.
- Por meio do Suporte Lenovo Line, é possível obter assistência técnica, mediante cobrança, para problemas de uso, configuração e software com os produtos Lenovo.

  Para localizar os números de telefone de suporte local e gratuito, consulte o Site da lista de telefones de suporte. Você pode discar o número que localizar para sua área geográfica ou clicar em **Fale conosco** na página da Web para obter assistência.

  Para problemas com gravidade 1, a equipe de suporte funciona dia e noite. Para todas as outras gravidades, os horários de funcionamento e idiomas estão listados na página da Web para sua área geográfica.

  Para entrar em contato com o suporte de produtos na China, consulte o Lenovo Services – Site da China. Você também pode ligar para 400-106-8888 para obter suporte de produtos. O suporte telefônico está disponível de segunda a sexta, das 9h às 18h.

Capítulo 2. Exibindo alertas, eventos e trabalhos

O Lenovo XClarity Administrator fornece vários métodos que você pode usar para monitorar o status de dispositivos gerenciados.

- A lista de alertas fornece uma exibição em tempo real de problemas que foram identificados com o XClarity Administrator ou quaisquer dispositivos gerenciados.
- O log de auditoria e o log de eventos fornecem uma exibição histórica de ações de usuários e ações de eventos que foram identificadas pelo XClarity Administrator.
- O log de trabalhos fornece uma lista de tarefas em execução mais longas que foram executadas em um ou mais dispositivos gerenciados.

Colocando dispositivos no modo de manutenção

Quando um dispositivo está no modo de manutenção, o Lenovo XClarity Administrator exclui todos os eventos e alertas para esse dispositivo de todas as páginas em que os eventos e alertas são exibidos. Os alertas excluídos ainda são registrados em log, mas são ocultos na exibição.

Sobre esta tarefa

Apenas eventos e alertas gerados para um dispositivo enquanto o dispositivo estiver no modo de manutenção são excluídos. Os eventos e alertas gerados antes do dispositivo ser colocado no modo de manutenção, são exibidos.

Colocar um dispositivo gerenciado em manutenção e, em seguida, de volta ao serviço pode fazer com que o inventário desse dispositivo fique desatualizado. Se você vir anormalidades, atualize manualmente o inventário na página do dispositivo selecionando o dispositivo e clicando em **Todas as Ações → Inventário → Atualizar Inventário**.

Procedimento

Conclua uma das etapas a seguir para colocar os dispositivos no modo de manutenção.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Administração → Serviço e Suporte**. A página Serviço e Suporte é exibida.

Etapa 2. Clique em **Ações de Terminal** na navegação esquerda para exibir a página Ações de Terminal.

Etapa 3. Selecione um ou mais dispositivos para colocar no modo de manutenção.

Etapa 4. Clique em **Ações → Manutenção** para exibir a caixa de diálogo Mono de manutenção.

Etapa 5. Selecione a data e hora para tirar o dispositivo do modo de manutenção e coloque-o de volta em serviço.

Selecione **Indefinidamente** se não desejar que o dispositivo seja colocado novamente em serviço.

Etapa 6. Clique em **Confirmar**. A coluna de manutenção na tabela muda para Sim para esse dispositivo.

Depois de concluir

Quando você tiver concluído a manutenção no dispositivo, poderá colocar o dispositivo novamente em serviço selecionando o dispositivo e clicando em **Ações → Manutenção** e, em seguida, clicando em **Desativar manutenção** na caixa de diálogo. Se você não colocar manualmente o dispositivo novamente no

© Copyright Lenovo 2015, 2025

modo de serviço, ele será colocado no modo de serviço automaticamente depois que a data e a hora de término especificadas expirarem.

Trabalhando com alertas

Alertas são condições de hardware ou de gerenciamento que requerem análise e ação do usuário. O Lenovo XClarity Administrator sonda os dispositivos gerenciados assincronicamente e exibe os alertas que são recebidos desses dispositivos.

Sobre esta tarefa

Saiba mais: XClarity Administrator: monitoramento

Normalmente, quando um alerta é recebido, um evento correspondente é armazenado no log de eventos. É possível ter um alerta sem um evento correspondente no log de eventos (mesmo se o log for fechado). Por exemplo, os eventos que ocorrem antes de gerenciar um chassi não são exibidos no log de eventos. Entretanto, os alertas do chassi são exibidos no log de alertas porque o Lenovo XClarity Administrator sonda o CMM após o chassi ser gerenciado.

Visualizando alertas ativos

É possível exibir uma lista de todos os alertas ativos de hardware e de gerenciamento.

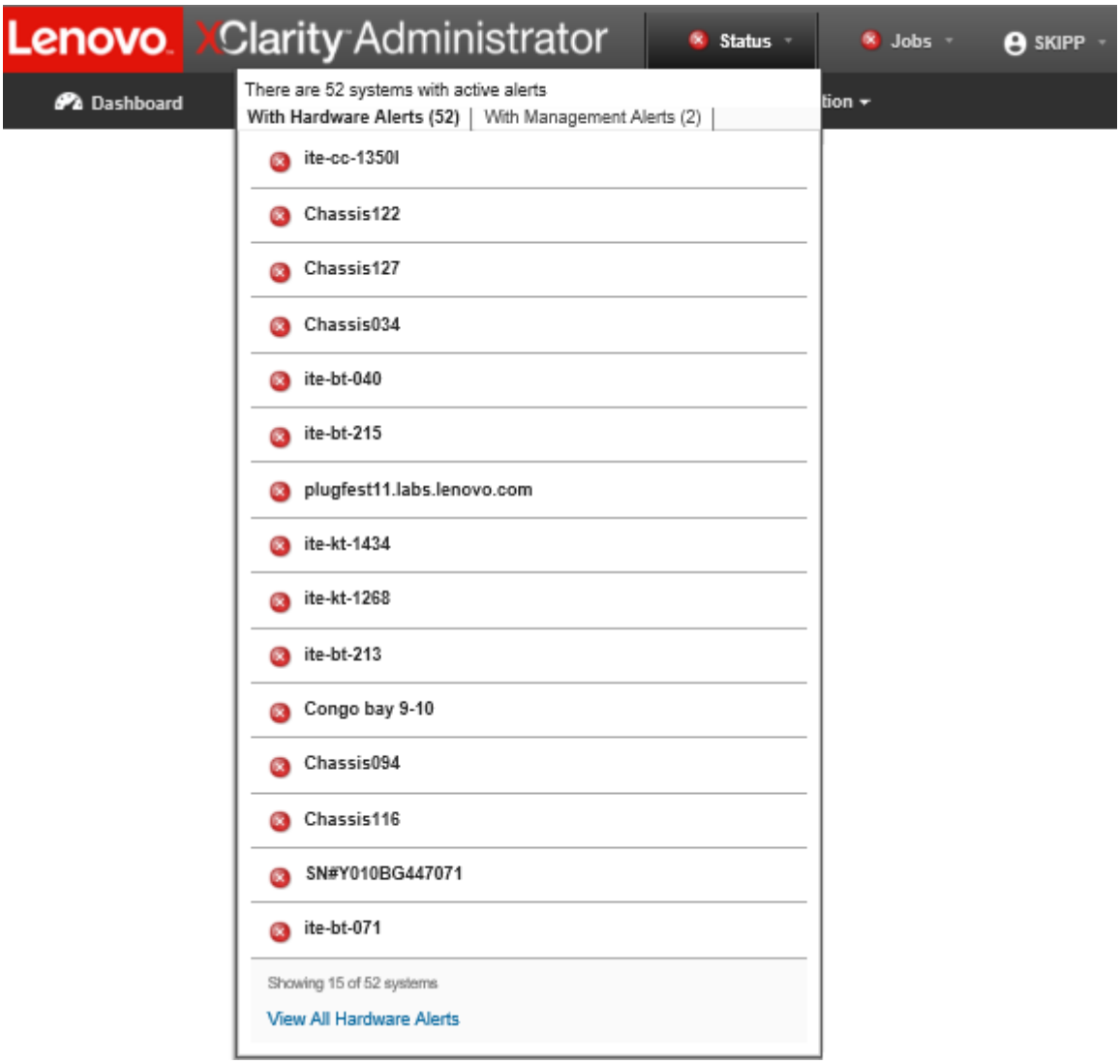
Sobre esta tarefa

Nota: Os alertas de dispositivos Lenovo Storage são apresentados apenas em inglês, mesmo quando o local de Lenovo XClarity Administrator é configurado em outro idioma. Use um sistema externo de tradução para traduzir manualmente as mensagens, se necessário.

Procedimento

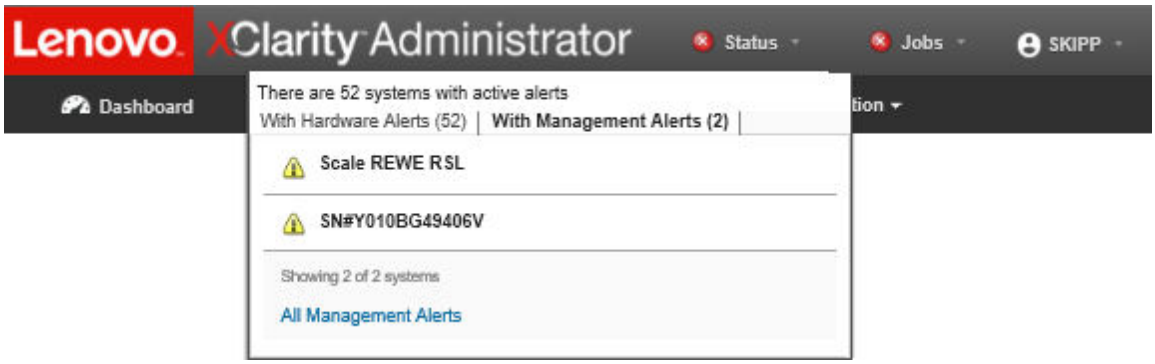
Conclua um desses procedimentos para exibir os alertas ativos.

- Para exibir apenas alertas de dispositivos gerenciados (conhecidos como *alertas de hardware*):
  1. Na barra de título do XClarity Administrator, clique no menu suspenso **Status** para exibir um resumo dos alertas de hardware e de gerenciamento.
  2. Clique na guia **Com Alertas de Hardware** para ver um resumo de alertas para cada dispositivo gerenciado.



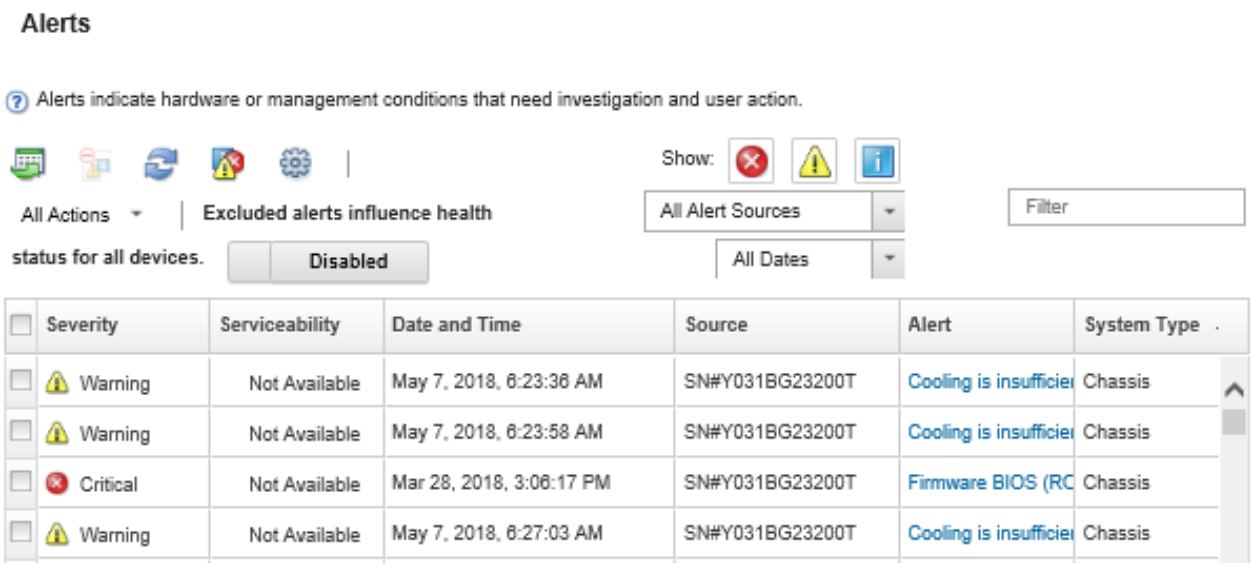
3. Passe o cursor sobre um dispositivo que esteja listado nessa guia para exibir uma lista de alertas desse dispositivo.
4. Clique no link **Todos os Alertas de Hardware** para exibir a página Alertas com uma lista filtrada de todos os alertas de hardware.

- Para exibir apenas alertas do XClarity Administrator (conhecidos como *alertas de gerenciamento*):
  1. Na barra de título do XClarity Administrator, clique no menu suspenso **Status** para exibir um resumo dos alertas de hardware e de gerenciamento.
  2. Clique na guia **Com Alertas de Gerenciamento** para ver um resumo de todos os alertas do CMM e do XClarity Administrator.



3. Passe o cursor sobre um dispositivo que esteja listado nessa guia para exibir uma lista de alertas desse dispositivo.
4. Clique no link **Todos os Alertas de Gerenciamento** para exibir a página Alertas com uma lista filtrada de todos os alertas do CMM e do XClarity Administrator.

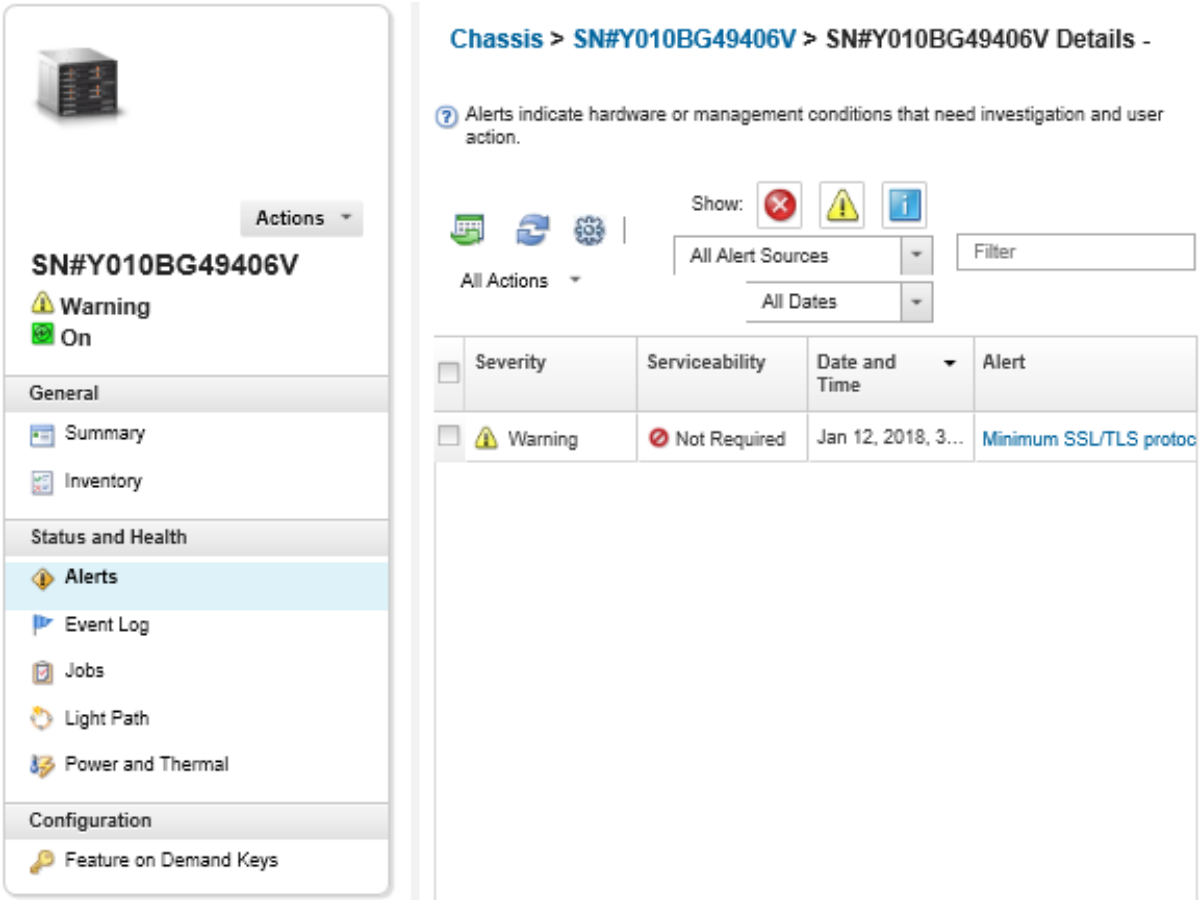
- Para exibir todas os alertas no XClarity Administrator, clique em **Monitoramento → Alertas** na barra de menu do XClarity Administrator. A página Alertas é exibida com uma lista de todos os alertas ativos.



- Para exibir alertas de um dispositivo específico:
  1. Na barra de menu do XClarity Administrator, clique em **Hardware** e clique em um tipo de dispositivo. É exibida uma página com uma exibição tabular de todos os dispositivos gerenciados desse tipo. Por exemplo, clique em **Hardware → Servidores** para exibir a página Servidores.
  2. Clique em um dispositivo específico para exibir a página Resumo do dispositivo.
  3. Em Status e Funcionamento, clique em **Alertas** para exibir uma lista de todos os alertas associados a esse dispositivo.

     Notas: A coluna Capacidade de Manutenção poderá mostrar "Não Disponível" se:

     – O alerta no dispositivo ocorrer antes de XClarity Administrator iniciar o gerenciamento
     – O log de eventos tiver sido encapsulado e o evento associado a esse alerta não estiver mais no log de eventos.



Resultados

Na página Alertas, é possível executar as ações a seguir:

- Atualizar a lista de alertas clicando no ícone **Atualizar** ( ).

  Dica: se novos alertas forem detectados, o log de alertas será atualizado automaticamente a cada 30 segundos.
- Visualize informações sobre um alerta específico (incluindo uma explicação e uma ação do usuário) e sobre o dispositivo que é a origem do alerta (como o identificador exclusivo universalmente) clicando no link na coluna **Alerta**. Uma caixa de diálogo com informações sobre as propriedades e detalhes de alerta é exibida.

  Nota: Se a explicação e as ações de recuperação de um alerta não forem exibidas na guia **Detalhes**, vá até Documentação online do Lenovo Flex System e procure o ID do alerta (por exemplo, `FQXHMSE0004G`). O website sempre fornece as informações mais atualizadas.
- Por padrão, os alertas excluídos não influenciam o status de integridade dos dispositivos gerenciados. Você pode permitir que os alertas excluídos influenciem o status de funcionamento de dispositivos gerenciados na página Alertas clicando em Alternar para ativar **Alertas excluídos influenciam o status de funcionamento de todos os dispositivos**.
- É possível configurar preferências de limite para gerar um alerta e um evento quando um determinado valor, como a vida útil de um SSD em um servidor ThinkSystem ou ThinkServer excede um nível crítico ou de aviso (consulte Configurando preferências de limite para gerar alertas e eventos na documentação online do XClarity Administrator).

- Exportar o log de alertas clicando no ícone **Exportar como CSV** ( ).

  Nota: Os registros de data e hora no log exportado usam a hora local que é especificada pelo navegador da Web.
- Excluir alertas específicos de todas as páginas em que eles são exibidos (consulte Excluindo alertas).
- Refinar a lista de alertas que são exibidos na página atual:
  - Mostrar ou ocultar alertas de uma determinada gravidade clicando nos seguintes ícones:
    - Ícone **Alertas críticos** ( )
    - Ícone **Alertas de avisos** ( )
    - Ícone **Alertas informativos** ( )
  - Mostrar alertas somente de origens específicas. É possível escolher uma das opções a seguir na lista suspensa:
    - Todas as Fontes de Alertas
    - Eventos de Hardware
    - Eventos de Gerenciamento
    - Eventos do Centro de Manutenção
    - Eventos com Possibilidade de Manutenção pelo Cliente
    - Eventos que não permitem manutenção
  - Mostrar apenas alertas com uma data e hora específicas. É possível escolher uma das opções a seguir na lista suspensa:
    - Todas as Datas
    - Duas horas anteriores
    - 24 horas anteriores
    - Semana Passada
    - Mês Passado
  - Listar apenas alertas que contêm o texto específico inserindo o texto no campo **Filtro**.
  - Classificar os alertas por coluna clicando em um título de coluna.

Excluindo alertas

Se houver alertas específicos que não são de seu interesse, será possível excluí-los de todas as páginas em que os alertas são exibidos. Os alertas excluídos ainda estão no log, mas são ocultos em todas as páginas em que alertas são exibidos, incluindo visualizações de log e status do dispositivo.

Sobre esta tarefa

Os alertas excluídos são ocultos para todos os usuários, não apenas para o usuário que define a configuração.

É possível colocar os dispositivos no modo de manutenção para que todos os eventos e alertas para esses dispositivos sejam excluídos (consulte Colocando dispositivos no modo de manutenção).

Restrição: Apenas usuários com autoridade de administrador podem restaurar ou excluir alertas.

Importante: Se você excluir alertas de status, o status do dispositivo no resumo e as páginas detalhadas não mudarão.

ProcedimentoComplete as etapas a seguir para excluir alertas do log de alertas.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Monitoramento → Alertas**. A página Alertas é exibida.

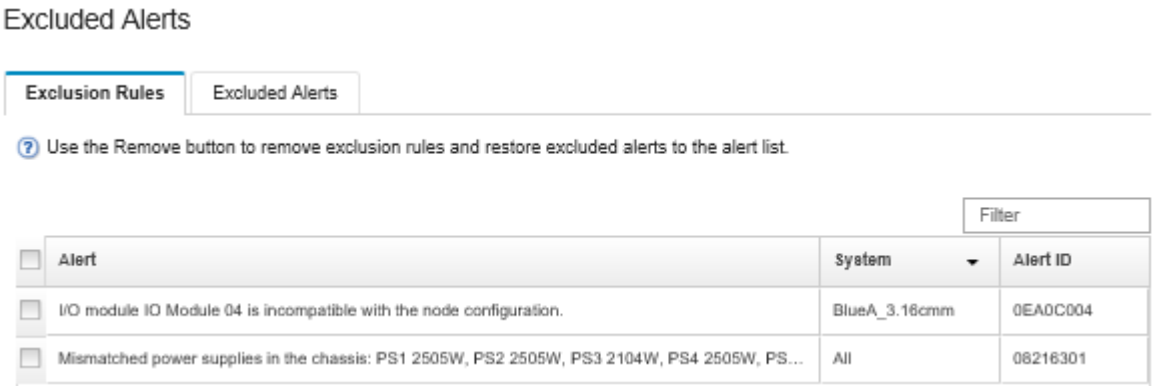
Etapa 2. Selecione os alertas a serem excluídos, e clique no ícone **Excluir alertas** ( ). A caixa de diálogo de Excluir alertas é exibida.

Etapa 3. Selecione uma das opções a seguir:
- **Excluir alertas selecionados de todos os sistemas**. Exclui os alertas selecionados de todos os dispositivos gerenciados.
- **Excluir alertas somente de sistemas no escopo da instância selecionada**. Exclui os alertas selecionados dos dispositivos gerenciados aos quais os alertas selecionados se aplicam.

Etapa 4. Clique em **Salvar**.

Depois de concluir

Quando você exclui alertas, o Lenovo XClarity Administrator cria regras de exclusão baseadas nas informações fornecidas. É possível exibir uma lista de regras de exclusão e de alertas excluídos na página Alertas clicando no ícone **Mostrar alertas excluídos/confirmados** ( ). Na caixa de diálogo Alertas excluídos/confirmados, clique na guia **Regras de exclusão** para exibir a lista de regras de exclusão ou clique na guia **Alertas excluídos** para exibir a lista de alertas excluídos.



Por padrão, os alertas excluídos não influenciam o status de integridade dos dispositivos gerenciados. Você pode permitir que os alertas excluídos influenciem o status de funcionamento de dispositivos gerenciados na página Alertas clicando em Alternar para ativar **Mostrar alertas excluídos/confirmados**.

É possível restaurar os alertas que foram excluídos no log de alertas removendo a regra de exclusão apropriada. Para remover uma regra de exclusão, clique no ícone **Mostrar Alertas Excluídos** ( ) para exibir a caixa de diálogo Alertas Excluídos, selecione as regras de exclusão ou o alerta excluído a serem restaurados e clique em **Remover**.

Resolvendo um alerta

O Lenovo XClarity Administrator fornece informações sobre as ações apropriadas a serem executadas para resolver um alerta.

Procedimento

Conclua as seguintes etapas para resolver um alerta.

Etapa 1. Na barra de menu Lenovo XClarity Administrator, clique em **Monitoramento → Alertas** para exibir a página Alertas.

Etapa 2. Localize o alerta no log de alertas.

Etapa 3. Clique no link na coluna **Alerta** para exibir informações sobre o alerta (incluindo uma explicação e ações de recuperação) e as propriedades do dispositivo que é a origem de alerta (como o identificador exclusivo universalmente).

Etapa 4. Conclua as ações de recuperação listadas na guia **Detalhes** para resolver o alerta. O exemplo a seguir ilustra ações de recuperação para um evento.

Altere a configuração de política de segurança no chassi gerenciado referenciado para corresponder à política de segurança atual no servidor de gerenciamento.

Para alterar a política de segurança no chassi, abra uma sessão da interface da linha de comandos no Chassis Management Module (CMM) e execute um dos seguintes comandos:

- Para alterar o nível de política de segurança para `Secure`:
  `security -p secure -T mm[p]`
- Para alterar o nível de política de segurança para `Legacy`:
  `security -p legacy -T mm[p]`

Nota: Se a explicação e as ações de recuperação de um alerta não forem exibidas na guia **Detalhes**, vá até Documentação online do Lenovo Flex System e procure o ID do alerta (por exemplo, `FQXHMSE0004G`). O website sempre fornece as informações mais atualizadas.

Se você seguir as ações recomendadas e o problema persistir, entre em contato com Suporte da Lenovo.

Confirmando alertas

Quando um alerta ativo é confirmado, ele é listado em páginas em que os alertas são exibidos, mas não afeta o status de gravidade do dispositivo aplicável.

Procedimento

Conclua as etapas a seguir para confirmar um alerta.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Monitoramento → Alertas**. A página Alertas é exibida.

Etapa 2. Selecione os alertas a serem confirmados.

Etapa 3. Clique no ícone **Confirmar alertas** ( ).

Depois de concluir

- É possível exibir uma lista de alertas confirmados na página Alerts (Alertas) clicando no ícone **Mostrar alertas excluídos/confirmados** ( ) para exibir a caixa de diálogo Excluded/Acknowledged Alerts (Alertas excluídos/confirmados) e, em seguida, clicando na guia **Alertas confirmados**.
- É possível remover a confirmação de um alerta ativo clicando no ícone **Mostrar alertas excluídos/confirmados** ( ) para exibir a caixa de diálogo Alertas excluídos/confirmados e, em seguida, clicando na guia **Alertas confirmados**, selecione os alertas e clique no ícone **Remover confirmação** ( ).

Trabalhando com eventos

No Lenovo XClarity Administrator, você terá acesso a um log de eventos e um log de auditoria.

Sobre esta tarefa

Saiba mais: XClarity Administrator: monitoramento

O *log de evento* fornece uma lista histórica de todos os hardwares e eventos gerenciados.

O *log de auditoria* fornece um registro histórico das ações do usuário, como fazer login no Lenovo XClarity Administrator, criar um novo usuário e alterar uma senha de usuário. É possível usar o log de auditoria para acompanhar e documentar a autenticação e controles nos sistemas de TI.

Monitorando eventos no log de eventos

O *log de evento* fornece uma lista histórica de todos os hardwares e eventos gerenciados.

Sobre esta tarefa

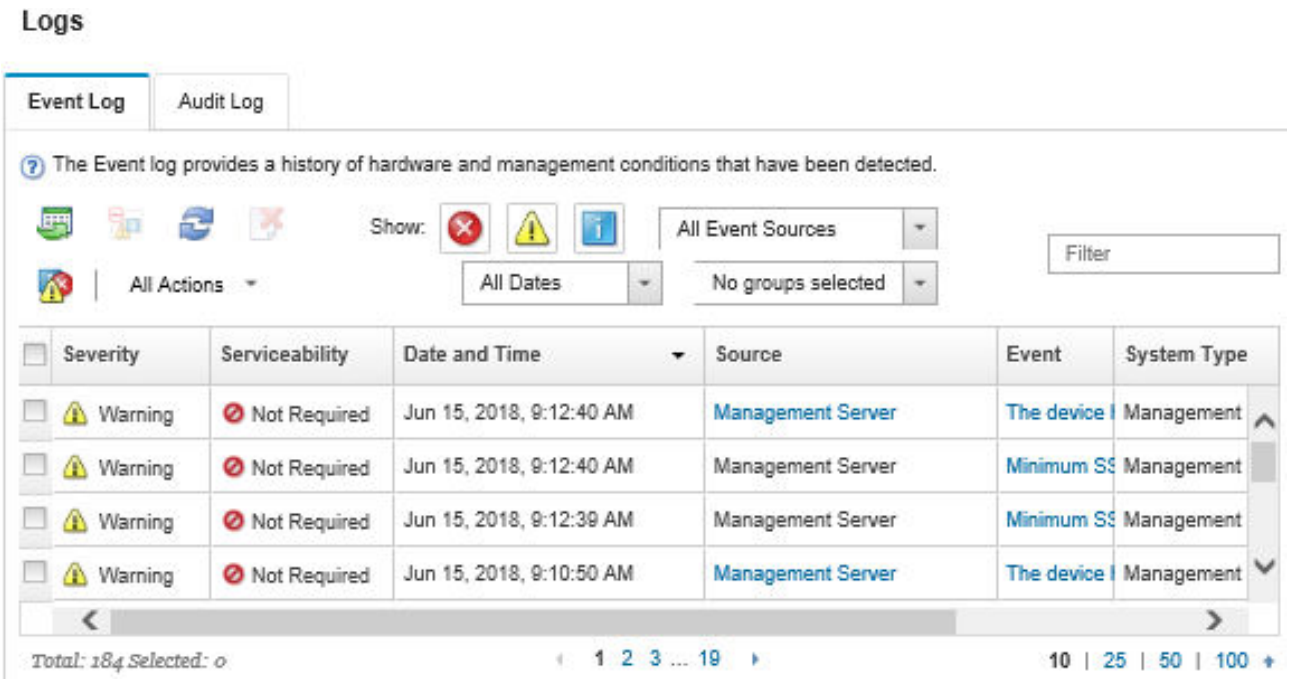
O log de evento contém eventos informativos e não informativos. O número de cada um destes eventos variam até, no máximo, 50.000 eventos ser atingido no log de eventos. Nesse ponto, há um máximo de 25.000 eventos informativos e 25.000não informativos sem informações e eventos informativos. Por exemplo, há 0 eventos no log de eventos inicialmente. Suponha que os eventos são recebidos e que 20.000 eventos informativos e 30.000 eventos não informativos são recebidos. Quando o evento seguinte é recebido, o evento informativo mais antigo será descartado se um evento não informativo for mais antigo. Finalmente, o log equilibra para que haja 25.000 de cada tipo de evento.

O Lenovo XClarity Administrator envia um evento quando o log de evento atinge 80% de seu tamanho mínimo e outro evento quando a soma de logs de evento e auditoria atingem 100% de seu tamanho máximo.

Dica: você pode exportar o log de evento para certificar-se de ter um registro completo de todos os hardwares e eventos de gerenciamento. Para exportar o log de evento, clique no ícone **Exportar como CSV** ( ).

Procedimento

Para exibir o log de evento, clique em **Monitoramento → Logs de Evento** na barra de menu do Lenovo XClarity Administrator e clique na guia **Log de Evento**. A página Log de Eventos é exibida.



A coluna **Capacidade de Manutenção** identifica se o dispositivo requer o serviço. Esta coluna pode conter um dos seguintes valores:

- **Não necessário**. O evento é informativo e não requer o serviço.
- **Usuário**. Toma ação de recuperação apropriada para resolver o problema.

  Para exibir informações sobre um evento específico, clique no link na coluna **Evento**. Uma caixa de diálogo é exibida com informações sobre as propriedades do dispositivo que enviou o evento, detalhes sobre o evento e as ações de recuperação.
- **Suporte**. Se o Call Home é habilitado no Lenovo XClarity Administrator, o evento é enviado geralmente ao Centro de Suporte da Lenovo, a menos que já exista um tíquete de serviço aberto para o mesmo ID do evento para o dispositivo.

  Se o Call Home não estiver ativado, é recomendável abrir manualmente um tíquete de serviço para resolver o problema (consulte Abrindo um tíquete de serviço na documentação online do Lenovo XClarity Administrator).

Resultados

Na página Log de Evento, é possível executar as ações a seguir:

- Exibir a origem do evento, clicando no link na coluna **Fonte**.
- Atualizar a lista de eventos clicando no ícone **Atualizar** ( ).

  Dica: O log de evento será atualizado automaticamente a cada 30 segundos se novos eventos forem detectados.
- Limpar todos os eventos no log de eventos, selecionando **Todas as Ações → Limpar o log de eventos**.
- Exibir detalhes sobre um evento específico, clicando no link na coluna **Evento** e clicando na guia **Detalhes**.
- Exportar o log de evento clicando no ícone **Exportar como CSV** ( ).

  Nota: Os registros de data e hora no log exportado usam a hora local que é especificada pelo navegador da Web.
- Excluir eventos específicos de todas as páginas em que os eventos são exibidos (consulte Excluindo eventos).
- Refinar a lista de hardwares e eventos de gerenciamento que são exibidos na página atual:
  - Mostrar ou ocultar eventos de uma determinada gravidade clicando nos seguintes ícones na lista suspensa:
    - Ícone **Eventos críticos** ( )
    - Ícone **Eventos de avisos** ( )
    - Ícone **Eventos informativos** ( )
  - Mostrar eventos somente de origens específicas. É possível escolher uma das opções a seguir na lista suspensa:
    - Todas as Fontes de Alertas
    - Eventos de Hardware
    - Eventos de Gerenciamento
    - Eventos que Permitem Manutenção
    - Eventos com Possibilidade de Manutenção pelo Cliente
    - Eventos que não permitem manutenção
  - Mostrar apenas eventos com uma data e hora específicas. É possível escolher uma das opções a seguir:

  - Todas as Datas
  - 2 horas anteriores
  - 24 horas anteriores
  - Semana Passada
  - Mês Passado
  - Custom

  Se você selecionar **Personalizar**, poderá filtrar os eventos de hardware e de gerenciamento que foram gerados entre uma data de início personalizada e a data atual.
- Listar apenas eventos que contêm o texto específico inserindo o texto no campo **Filtro**.
- Classificar os eventos por coluna clicando em um título de coluna.

Monitorando eventos no log de auditoria

O *log de auditoria* fornece um registro histórico das ações do usuário, como fazer login no Lenovo XClarity Administrator, criar um novo usuário e alterar uma senha de usuário. É possível usar o log de auditoria para acompanhar e documentar a autenticação e controles nos sistemas de TI.

Sobre esta tarefa

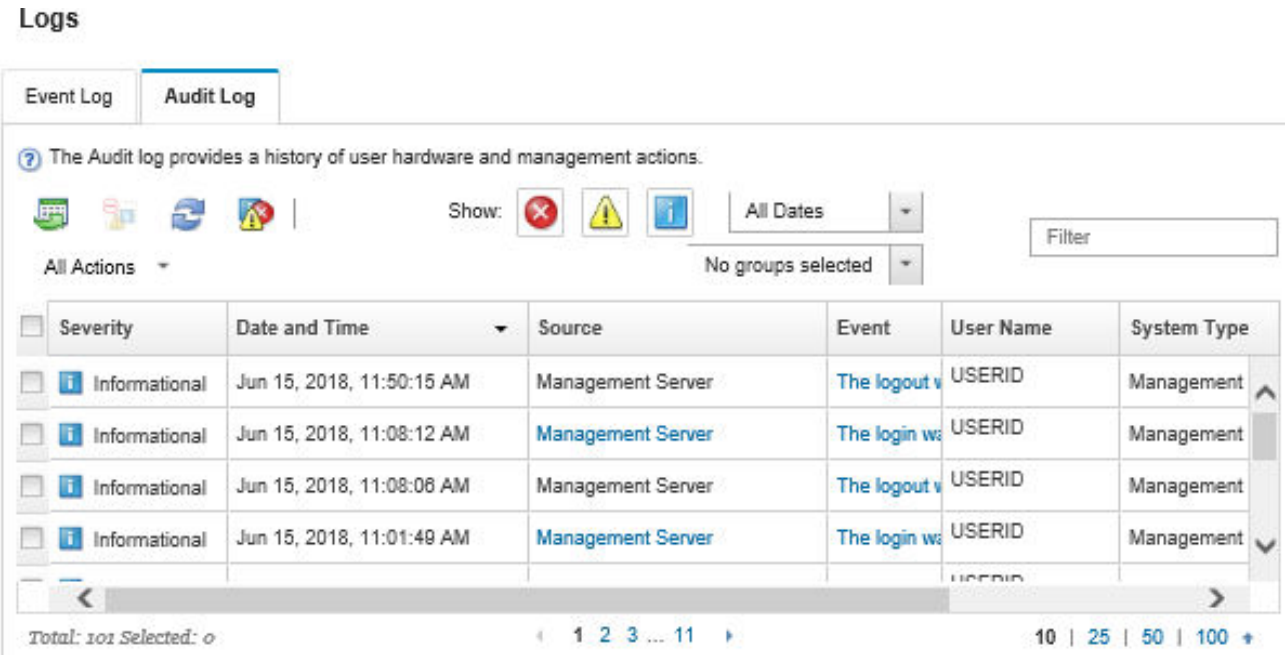
O log de auditoria pode conter um máximo de 50.000 eventos. Quando o tamanho máximo for atingido, o evento mais antigo em log será descartado e um novo evento será incluído no log.

O XClarity Administrator envia um evento quando o log de auditoria atinge 80% de seu tamanho máximo e outro evento quando a soma de logs de evento e auditoria atingem 100% de seu tamanho máximo.

Dica: você pode exportar o log de auditoria para certificar-se de ter um registro completo de todos os eventos de auditoria. Para exportar o log de auditoria, clique no ícone **Exportar como CSV** ( ).

Procedimento

Para exibir o log de auditoria, clique em **Monitoramento → Logs de Evento** na barra de menu do XClarity Administrator e clique na guia **Log de Auditoria**. A página Log de Auditoria é exibida.



Para exibir informações sobre um evento de auditoria específico, clique no link na coluna **Evento**. Uma caixa de diálogo é exibida com informações sobre as propriedades do dispositivo que enviou o evento, detalhes sobre o evento e as ações de recuperação.

Resultados

Nesta página, é possível executar as ações a seguir:

- Exibir a origem do evento de auditoria, clicando no link coluna **Fonte**.
- Atualizar a lista de eventos de auditoria, clicando no ícone **Atualizar** ( ).

  Dica: O log de evento será atualizado automaticamente a cada 30 segundos se novos eventos forem detectados.
- Exibir detalhes sobre um evento de auditoria específico, clicando no link na coluna **Evento** e, em seguida, clicando na guia **Detalhes**.
- Exportar o log de auditoria clicando no ícone **Exportar como CSV** ( ).

  Nota: Os registros de data e hora no log exportado usam a hora local que é especificada pelo navegador da Web.
- Excluir eventos de auditoria específicos de todas as páginas em que os eventos são exibidos (consulte Excluindo eventos).
- Refinar a lista de eventos de auditoria que são exibidos na página atual:
  - Mostrar ou ocultar eventos de uma determinada gravidade clicando nos seguintes ícones:
    - Ícone **Eventos críticos** ( )
    - Ícone **Eventos de avisos** ( )
    - Ícone **Eventos informativos** ( )
  - Mostrar apenas eventos com uma data e hora específicas. É possível escolher uma das opções a seguir na lista suspensa:
    - Todas as Datas
    - 2 horas anteriores
    - 24 horas anteriores
    - Semana Passada
    - Mês Passado
    - Custom

    Se você selecionar **Personalizar**, poderá filtrar os eventos de hardware e de gerenciamento que foram gerados entre uma data de início personalizada e a data atual.
  - Listar apenas eventos que contêm o texto específico inserindo o texto no campo **Filtro**.
  - Classificar os eventos por coluna clicando em um título de coluna.

Resolvendo um evento

O Lenovo XClarity Administrator fornece informações sobre as ações apropriadas a serem executadas para resolver um evento.

Procedimento

Conclua as seguintes etapas para resolver um evento.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Monitoramento → Logs de Eventos** para exibir a página Logs.

Etapa 2. Clique na guia **Log de Eventos**.

Etapa 3. Localize o evento no log de eventos.

Etapa 4. Clique no link na coluna **Evento** para exibir informações sobre esse evento (incluindo uma explicação e ações de recuperação) e sobre o dispositivo que é a origem do evento.

Etapa 5. Clique na guia **Detalhes**.

Etapa 6. Conclua as ações de recuperação no guia **Detalhes** para resolver o evento.

Nota: Se uma explicação e ação de recuperação para um evento não forem exibidas, acesse Documentação online do Lenovo Flex System e procure pelo título do evento. O website sempre fornece as informações mais atualizadas.

Se você seguir as ações recomendadas e o problema persistir, entre em contato com Suporte da Lenovo.

Excluindo eventos

Se houver eventos específicos que não são de seu interesse, será possível excluí-los de todas as páginas as quais os eventos são exibidos. Eventos excluídos continuam no log, mas são ocultos das páginas as quais os eventos são exibidos.

Sobre esta tarefa

Os eventos excluídos são ocultos para todos os usuários, não apenas para o usuário que define a configuração.

É possível colocar os dispositivos no modo de manutenção para que todos os eventos e alertas para esses dispositivos sejam excluídos (consulte Colocando dispositivos no modo de manutenção).

Restrição: apenas usuários com autoridade de administrador podem restaurar ou excluir eventos.

Procedimento

Complete as etapas a seguir para excluir eventos dos logs de eventos:

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Monitoramento → Logs de Eventos** e clique na guia **Log de Eventos**. Os Logs de Eventos são exibidos.

Etapa 2. Selecione os eventos a serem excluídos, e clique no ícone **Excluir eventos** ( ). A caixa de diálogo de Excluir Eventos é exibida.

Etapa 3. Selecione uma das opções a seguir:
- **Excluir eventos selecionados de todos os sistemas**. Exclui os eventos selecionados de todos os dispositivos gerenciados.
- **Excluir eventos somente de sistemas no escopo da instância selecionada**. Exclui os eventos selecionados dos dispositivos gerenciados os quais eventos selecionados se aplicam.

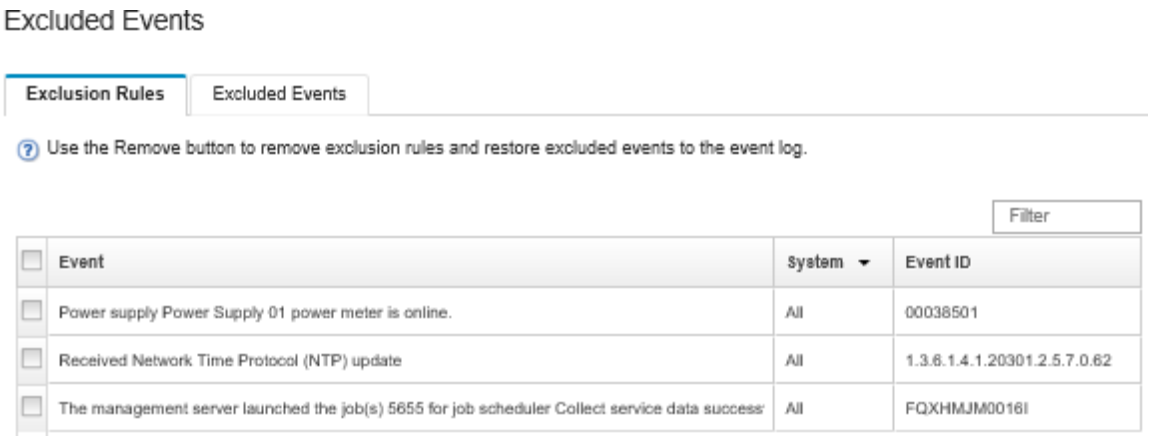
Etapa 4. Clique em **Salvar**.

Depois de concluir

Quando você exclui eventos, o Lenovo XClarity Administrator cria regras de exclusão baseadas em informações fornecidas.

- Exiba uma lista de regras de exclusão e de eventos excluídos na página de Logs, clicando no ícone **Mostrar Eventos Excluídos** ( ). Na caixa de diálogo Eventos excluídos, clique na guia **Regras de**

Exclusão para exibir as regras de exclusão ou clique na guia **Eventos Excluídos** para exibir os eventos excluídos.



- Restaure os eventos que foram excluídos no log de eventos removendo a regra de exclusão apropriada.

  Para remover uma regra de exclusão, clique no ícone **Mostrar Eventos Excluídos** ( ) para exibir a caixa de diálogo Eventos Excluídos, selecione as regras de exclusão a serem restauradas e clique em **Remover Exclusões**.
- Impeça os eventos que permitem manutenção que estão na lista de eventos excluídos de abrir relatórios de problemas automaticamente clicando em **Administração → Serviço e Suporte** na barra de menu do Lenovo XClarity Administrator, clicando na guia **Encaminhadores de Serviço** e selecionando **Não** ao lado da pergunta **Deseja que os eventos excluídos abram relatórios de problemas?**.

Encaminhamento de eventos

É possível configurar o Lenovo XClarity Administrator para encaminhar eventos para dispositivos móveis e aplicativos conectados instalados no seu ambiente para agregar e monitorar o status e o tempo de execução de hardware para seu ambiente de hardware.

Saiba mais: XClarity Administrator: monitoramento

Encaminhando eventos para o syslog, gerenciador SNMP remoto, e-mail e outros serviços de evento

É possível configurar o Lenovo XClarity Administrator para encaminhar eventos para aplicativos conectados instalados no seu ambiente para agregar e monitorar o status e o tempo de execução de hardware para seu ambiente de hardware. É possível definir o escopo de eventos para que sejam encaminhados com base no dispositivo, classe do evento, gravidade do evento e componente.

Sobre esta tarefa

O Lenovo XClarity Administrator pode encaminhar eventos para um ou mais dispositivos. Para eventos de auditoria, será possível escolher encaminhar todos os eventos de auditoria ou nenhum. Não é possível encaminhar eventos específicos de auditoria. Para eventos de hardware e de gerenciamento, é possível escolher encaminhar os eventos para uma ou mais severidades (crítico, aviso e informativo) e para um ou mais componentes (tais como unidades de disco, processadores e adaptadores).

O Lenovo XClarity Administrator usa encaminhadores de eventos para encaminhar eventos. Um *encaminhador de evento* inclui informações sobre o protocolo a ser usado, o destinatário, os dispositivos a serem monitorados e os eventos a serem encaminhados. Depois de criar e habilitar um encaminhador de evento, o Lenovo XClarity Administrator inicia o monitoramento para eventos recebidos com base em

critérios de filtro. Quando uma correspondência é encontrada, o protocolo associado é usado para encaminhar o evento.

Os seguintes protocolos são suportados:

- **Análise de Log do Azure**. O Lenovo XClarity Administrator encaminha os eventos monitorados pela rede para o Microsoft Azure Log Analytics.
- **E-mail**. O Lenovo XClarity Administrator encaminha os eventos monitorados para um ou mais endereços de e-mail usando SMTP. O e-mail contém informações sobre o evento, nome de host do dispositivo de origem e vinculá-lo a interface da Web Lenovo XClarity Administrator e ao aplicativo Lenovo XClarity Mobile.
- **FTP**. Encaminha os eventos monitorados pela rede para um servidor FTP.
- **REST**. O Lenovo XClarity Administrator encaminha os eventos monitorados pela rede para um serviço da Web REST.
- **SNMP**. O Lenovo XClarity Administrator encaminha os eventos monitorados na rede para um gerenciador SNMP remoto. Os traps SNMPv1 e SNMPv3 são suportados.

  Para obter informações sobre o arquivo MIB (Management Information Base) que descreve os traps SNMP que o Lenovo XClarity Administrator gera, consulte arquivo lenovoMgrAlert.mib na documentação online do Lenovo XClarity Administrator.
- **Syslog**. O Lenovo XClarity Administrator encaminha os eventos monitorados na rede para um servidor de log central onde ferramentas nativas podem ser usadas para monitorar o syslog.

É possível criar e habilitar até 20 encaminhadores de evento para enviar eventos a destinatários específicos.

Se o XClarity Administrator for reinicializado após os encaminhadores de evento serem configurados, você deverá aguardar o servidor de gerenciamento para gerar novamente dados internos antes que os eventos sejam encaminhados corretamente.

Para XClarity Administrator v1.2.0 e posterior, os **Comutadores** são incluído na guia **Eventos** nas caixas de diálogo Novo Encaminhador de Eventos e Alterar Encaminhador de Eventos. Se você atualizou para 1.2.0 ou posterior de uma versão anterior, lembre-se de atualizar seus encaminhadores de evento para incluir ou excluir os eventos de RackSwitch conforme apropriado. Isso será necessário mesmo se você tiver marcado a caixa de seleção **Todos os Sistemas** para selecionar todos os dispositivos.

Nota: Os eventos não são entregues se, por exemplo, a conectividade entre Lenovo XClarity Administrator e o encaminhador de evento está inativa ou a porta está bloqueada.

Configurando o encaminhamento de evento para o Análise de Log do Azure

É possível configurar o Lenovo XClarity Administrator para encaminhar eventos específicos ao Análise de Log do Azure.

Sobre esta tarefa

É possível criar e habilitar até 20 encaminhadores de evento para enviar eventos a destinatários específicos.

Se o XClarity Administrator for reinicializado após os encaminhadores de evento serem configurados, você deverá aguardar o servidor de gerenciamento para gerar novamente dados internos antes que os eventos sejam encaminhados corretamente.

Nota: Para XClarity Administrator v1.2.0 e posterior, os **Comutadores** são incluído na guia **Eventos** nas caixas de diálogo Novo Encaminhador de Eventos e Alterar Encaminhador de Eventos. Se você atualizou para 1.2.0 ou posterior de uma versão anterior, lembre-se de atualizar seus encaminhadores de evento para

incluir ou excluir os eventos de RackSwitch conforme apropriado. Isso será necessário mesmo se você tiver marcado a caixa de seleção **Todos os Sistemas** para selecionar todos os dispositivos.

Procedimento

Conclua as etapas a seguir para criar um encaminhador de evento para o Análise de Log do Azure.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Encaminhamento de Evento**. A página Encaminhamento de Evento é exibida.

Etapa 2. Clique na guia **Encaminhamento de eventos**.

Etapa 3. Clique no ícone **Criar** ( ). A guia **Geral** da caixa de diálogo Novo Encaminhador de Evento é exibida.

Etapa 4. Selecione **Análise de Log Azure** como o tipo de encaminhador de evento e preencha as informações específicas do protocolo:

- Digite o nome e a descrição opcional para o encaminhador de evento.
- Insira a chave primária para a interface do Análise de Log do Azure.
- Insira o período de tempo limite (em segundos) para a solicitação. O padrão é 30 segundos.
- **Opcional**: Se a autenticação for necessária, selecione um dos tipos de autenticação a seguir:
  - **Básico**. Autentica ao servidor especificado usando o ID do usuário e senha especificados.
  - **Nenhum**. Nenhuma autenticação é usada.

Etapa 5. Clique em **Formato de saída** para escolher o formato de saída dos dados de evento a serem encaminhados. As informações variam para cada tipo de encaminhador de evento.

O formato de saída de exemplo a seguir é o formato padrão para destinatários do Análise de Log do Azure. Todas as palavras entre colchetes duplos são as variáveis que são substituídas por valores reais quando um evento é encaminhado. As variáveis disponíveis para destinatários do Análise de Log do Azure estão listadas na caixa de diálogo Formato de Saída.

```
{\"Msg\":\"[[EventMessage]]\",\"EventID\":\"[[EventID]]\",\"Serialnum\":
\"[[EventSerialNumber]]\",\"SenderUUID\":\"[[EventSenderUUID]]\",\"Flags\":
\"[[EventFlags]]\",\"Userid\":\"[[EventUserName]]\",\"LocalLogID\":
\"[[EventLocalLogID]]\",\"DeviceName\":\"[[DeviceFullPathName]]\",\"SystemName\":
\"[[SystemName]]\",\"Action\":\"[[EventAction]]\",\"FailFRUs\":
\"[[EventFailFRUs]]\",\"Severity\":\"[[EventSeverity]]\",\"SourceID\":
\"[[EventSourceUUID]]\",\"SourceLogSequence\":[[EventSourceLogSequenceNumber]],
\"FailSNs\":\"[[EventFailSerialNumbers]]\",\"FailFRUUUIDs\":
\"[[EventFailFRUUUIDs]]\",\"EventClass\":\"[[EventClass]]\",\"ComponentID\":
\"[[EventComponentUUID]]\",\"Mtm\":\"[[EventMachineTypeModel]]\",\"MsgID\":
\"[[EventMessageID]]\",\"SequenceNumber\":\"[[EventSequenceID]]\",\"TimeStamp\":
\"[[EventTimeStamp]]\",\"Args\":[[EventMessageArguments]],\"Service\":
\"[[EventService]]\",\"CommonEventID\":\"[[CommonEventID]]\",\"EventDate\":
\"[[EventDate]]\",\"EventSource\":\"[[EventSource]]\",\"DeviceSerialNumber\":
\"[[DeviceSerialNumber]]\",\"DeviceIPAddress\":\"[[DeviceIPAddress]]\",
\"LXCA\":\"[[LXCA_IP]]\"}
```

É possível clicar em **Redefinir para padrões** para alterar o formato de saída novamente para os campos padrão.

Etapa 6. Selecione **Permitir eventos excluídos** para evitar que eventos excluídos sejam encaminhados ou limpe **Permitir eventos excluídos** para encaminhar eventos excluídos. Para obter mais informações, consulte Excluindo eventos.

Etapa 7. Selecione **Habilitar este encaminhador** para ativar o encaminhamento de eventos para esse encaminhador.

Etapa 8. Clique em **Avançar** para exibir a guia **Dispositivos**.

Etapa 9. Selecione os dispositivos e os grupos que deseja monitorar para este encaminhador de evento.

Dica para encaminhar eventos para todos os dispositivos gerenciados (atuais e futuros), marque a caixa de seleção **Combinar todos os sistemas**.Se você não marcar a caixa de seleção **Combinar todos os sistemas**, certifique-se que os dispositivos selecionados não tenham um DUMMY-UUID na coluna UUID. Um Dummy-UUID é atribuído para dispositivos que ainda não se recuperaram após uma reinicialização ou não foram totalmente descobertos pelo servidor de gerenciamento. Se você selecionar um dispositivo com um Dummy-UUID, o encaminhamento de evento funcionará para este dispositivo até o ponto quando o dispositivo for descoberto ou recuperado, e o Dummy-UUID é alterado para o UUID real.

Etapa 10. Clique em **Avançar** para exibir a guia **Eventos**.

Etapa 11. Selecione os filtros a serem usados para este encaminhador de evento.

- **Corresponder por categoria de evento**
  1. Para encaminhar todos os eventos de auditoria independentemente do nível de status, selecione **Inclui todos os eventos de Auditoria**.
  2. Para encaminhar todos os eventos de garantia, selecione **Inclui eventos de Garantia**.
  3. Para encaminhar todos os eventos de alteração de status de funcionamento, selecione **Incluir eventos de alteração de status**.
  4. Para encaminhar todos os eventos de atualização de status de funcionamento, selecione **Incluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja encaminhar.
  6. Insira os IDs para um ou mais eventos que você deseja que o encaminhamento seja excluído. Separe os IDs usando uma vírgula (por exemplo, `FQXHMEM0214I,FQXHMEM0214I`).
- **Faça a correspondência por código de evento**. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe diversos IDs usando uma vírgula.
- **Excluir por categoria de evento**.
  1. Para excluir todos os eventos de auditoria independentemente do nível de status, selecione **Excluir todos os eventos de Auditoria**.
  2. Para excluir todos os eventos de garantia, selecione **Excluir eventos de Garantia**.
  3. Para excluir todos os eventos de alteração de status de funcionamento, selecione **Excluir eventos de alteração de status**.
  4. Para excluir todos os eventos de atualização de status de funcionamento, selecione **Excluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja excluir.
  6. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe os IDs usando uma vírgula.
- **Exclua por código de evento**. Insira os IDs de um ou mais eventos que você deseja excluir. Separe diversos IDs usando uma vírgula.

Etapa 12. Decida se deve incluir determinados tipos de eventos.

- **Incluir Todos os Eventos de Auditoria**. Envia notificações sobre eventos de auditoria, com base nas classes de eventos e gravidades selecionadas.
- **Incluir eventos de Garantia**. Envia notificações sobre garantias.
- **Incluir eventos de alteração de status**. Envia notificações sobre alterações no status.
- **Incluir eventos de atualização de status**. Enviou notificações sobre novos alertas
- **Incluir eventos do boletim**. Envia notificação sobre novos boletins.

Etapa 13. Selecione os tipos de eventos e as gravidades sobre os quais deseja ser notificado.

Etapa 14. Selecione se deve filtrar eventos por capacidade de manutenção.

Etapa 15. Clique em **Avançar** para exibir a guia **Planejador**.

Etapa 16. **Opcional:** Defina a hora e os dias em que deseja que os eventos especificados sejam encaminhados para este encaminhador de evento. Apenas eventos que ocorrem durante o slot de tempo especificado são encaminhados.

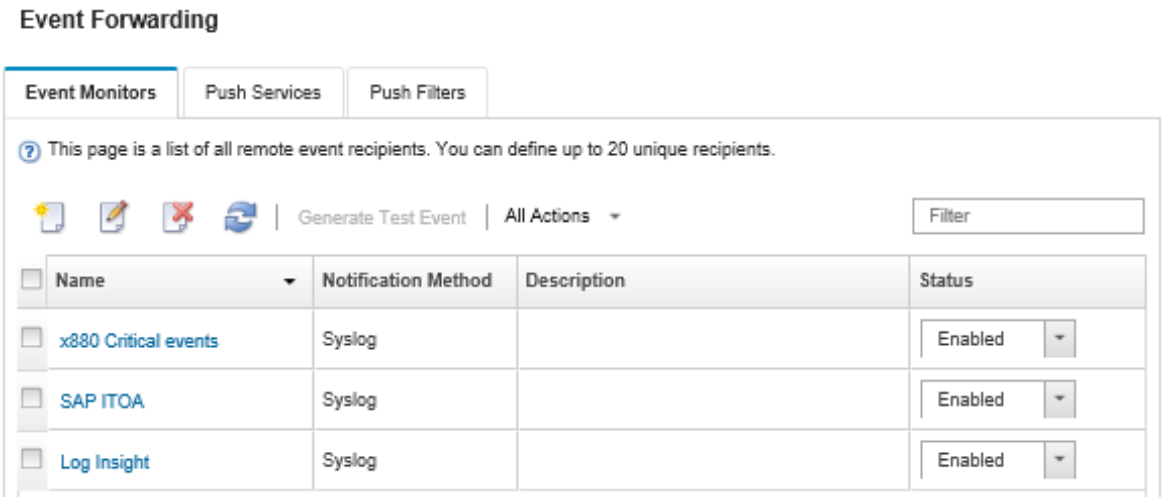
Se você não criar um planejamento para o encaminhador de evento, os eventos serão encaminhados 24h por dia/7 dias por semana.

1. Use o ícone **Rolar para a esquerda** (◀) e o ícone **Rolar para a direita** (▶), e os botões **Dia**, **Semana** e **Mês** para localizar o dia e a hora em que você deseja iniciar o planejamento.
2. Clique duas vezes no slot de tempo para abrir a caixa de diálogo Novo Período de Tempo.
3. Preencha as informações necessárias, incluindo a data e a hora de início e encerramento, e se está planejado para ocorrer novamente.
4. Clique em **Criar** para salvar o planejamento e fechar a caixa de diálogo. O novo planejamento é incluído no calendário.

Dica:
- É possível alterar o período arrastando a entrada de programação para outro período no calendário.
- É possível alterar a duração selecionando o início ou o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar o horário de encerramento selecionando o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar uma programação clicando duas vezes na entrada da programação no calendário e clicando em **Editar Entrada**.
- É possível exibir um resumo de todas as entradas da programação selecionando **Mostrar Resumo do Planejador**. O resumo inclui o período de cada entrada e quais entradas são repetíveis.
- É possível excluir uma entrada da programação do calendário ou do resumo planejador selecionando a entrada e clicando em **Excluir Entrada**.

Etapa 17. Clique em **Criar**.

O encaminhador de evento está listado na tabela Encaminhamento de Evento.



Etapa 18. Selecione o novo encaminhador de evento, clique em **Gerar Evento de Teste** e verifique se os eventos foram encaminhados corretamente para o servidor do Análise de Log do Azure apropriado.

Depois de concluir

Na página Encaminhamento de Evento, é possível executar as seguintes ações em um encaminhador de evento selecionado:

- Atualizar a lista de encaminhadores de evento clicando no ícone **Atualizar** ( ).
- Exibir detalhes sobre um encaminhador de evento específico, clicando no link na coluna **Nome**.
- Alterar as propriedades do encaminhador de evento e filtrar os critérios clicando no nome do encaminhador de evento na coluna **Nome**.
- Excluir o encaminhador de evento clicando no ícone **Excluir** ( ).
- Suspender o encaminhamento de evento (consulte Suspendendo o encaminhamento de evento).

Configurando o encaminhamento de evento em um serviço de e-mail usando SMTP

É possível configurar o Lenovo XClarity Administrator para encaminhar eventos específicos para um serviço de e-mail usando SMTP.

Antes de iniciar

Para encaminhar o e-mail para um serviço e-mail baseado na Web (como Gmail, Hotmail ou Yahoo), o servidor SMTP deve dar suporte ao encaminhamento do e-mail da Web.

Antes de configurar um encaminhador de eventos para um serviço da Web Gmail, revise as informações em Configurando o encaminhamento de evento para o syslog, gerenciador SNMP remoto ou e-mail na documentação online do Lenovo XClarity Administrator.

Sobre esta tarefa

É possível criar e habilitar até 20 encaminhadores de evento para enviar eventos a destinatários específicos.

Se o XClarity Administrator for reinicializado após os encaminhadores de evento serem configurados, você deverá aguardar o servidor de gerenciamento para gerar novamente dados internos antes que os eventos sejam encaminhados corretamente.

Nota: Para XClarity Administrator v1.2.0 e posterior, os **Comutadores** são incluído na guia **Eventos** nas caixas de diálogo Novo Encaminhador de Eventos e Alterar Encaminhador de Eventos. Se você atualizou para 1.2.0 ou posterior de uma versão anterior, lembre-se de atualizar seus encaminhadores de evento para incluir ou excluir os eventos de RackSwitch conforme apropriado. Isso será necessário mesmo se você tiver marcado a caixa de seleção **Todos os Sistemas** para selecionar todos os dispositivos.

Procedimento

Conclua as etapas a seguir para criar um encaminhador de evento para e-mail usando SMTP.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Encaminhamento de Evento**. A página Encaminhamento de Evento é exibida.

Etapa 2. Clique na guia **Encaminhamento de eventos**.

Etapa 3. Clique no ícone **Criar** ( ). A guia **Geral** da caixa de diálogo Novo Encaminhador de Evento é exibida.

Etapa 4. Selecione **E-mail** como o tipo de encaminhador de evento e preencha as informações específicas do protocolo:

- Digite o nome, o host de destino e a descrição opcional para o encaminhador do evento.
- Insira a porta a ser usada para o encaminhamento de eventos. O padrão é 25.
- Insira o período de tempo limite (em segundos) para a solicitação. O padrão é 30 segundos.

- Insira o endereço de e-mail para cada destinatário. Separe diversos endereços de e-mail usando uma vírgula.

  Para enviar o e-mail do contato de suporte atribuído para o dispositivo, selecione **Usar e-mail (s) do contato de suporte** (consulte Definindo os contatos de suporte de um dispositivo na documentação online do XClarity Administrator).
- **Opcional:** Insira o endereço de e-mail do remetente do e-mail (por exemplo, `john@company.com`).

  Se você não especificar um endereço de e-mail, o endereço do remetente será `LXCA.`<*source_identifier*>`@`<*smtp_host*> por padrão.

  Se você especificar apenas o domínio do remetente, o formato do endereço do remetente será <*LXCA_host_name*>@<*sender_domain*> (por exemplo, XClarity1@company.com).

  Notas:

  – Se você configurou o servidor SMTP para requerer um nome do host para encaminhar e-mails e não configurou um nome do host para XClarity Administrator, é possível que o servidor SMTP descarte os eventos encaminhados. Se o XClarity Administrator não tiver um nome do host, o evento será encaminhado com o endereço IP. Se o endereço IP não pode ser obtido, o "localhost" é enviado no seu lugar, o que pode fazer com que o servidor SMTP descarte o evento.

  – Se você especificar o domínio do remetente, a origem não identificará o endereço do remetente. Ao invés disso, as informações sobre a origem do evento serão incluídas no corpo do e-mail, incluindo o nome do sistema, endereço IP, tipo/modelo e o número de série.

  – Se o servidor SMTP só aceita e-mails que foram enviados por um usuário registrado, o endereço padrão do remetente (`LXCA.`<*source_identifier*>`@`<*smtp_host*>) é rejeitado. Nesse caso, você deve especificar pelo menos um nome de domínio no campo **Do endereço**.
- **Opcional:** Para estabelecer uma conexão segura com o servidor SMTP, selecione os tipos de conexão a seguir:
  – **SSL**. Usam o protocolo SSL durante a comunicação.
  – **STARTTLS**. Usa TLS para formar uma comunicação segura em um canal não seguro.

  Se um destes tipos de conexão for selecionado, o LXCA tentará baixar e importar o certificado do servidor SMTP para seu armazenamento confiável. Você é solicitado a aceitar a adição desse certificado ao armazenamento confiável.
- **Opcional:** Se a autenticação for necessária, selecione um dos tipos de autenticação a seguir:
  – **Regular**. Autentica ao servidor SMTP especificado usando o ID do usuário e senha especificados.
  – **NTLM**. Usa o protocolo NT LAN Manager (NTLM) para autenticação ao servidor SMTP especificado usando o ID do usuário, senha e nome de domínio especificados.
  – **OAUTH2**. Usa protocolo SASL (Simple Authentication and Security Layer) para autenticar o servidor SMTP especificado usando o nome de usuário e o token de segurança especificados. Normalmente, o nome do usuário é o seu endereço de e-mail.

    Atenção: O token de segurança expira após um curto período de tempo. É sua responsabilidade atualizar o token de segurança.
  – **Nenhum**. Nenhuma autenticação é usada.

Etapa 5. Clique em **Formato de saída** para escolher o formato de saída dos dados do evento a serem encaminhados no corpo do e-mail e o formato do assunto do e-mail. As informações variam para cada tipo de encaminhador de evento.

O formato de saída de exemplo a seguir é o formato padrão para destinatários do e-mail. Todas as palavras entre colchetes duplos são as variáveis que são substituídas por valores reais quando um

evento é encaminhado. As variáveis disponíveis para destinatários do e-mail estão listadas na caixa de diálogo Formato de Saída.

Assunto do e-mail

```
[[DeviceName]]-[[EventMessage]]
```

Corpo do e-mail

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name          : [[DeviceName]]\n
Product name         : [[DeviceProductName]]\n
Host name            : [[DeviceHostName]]\n
Machine Type         : [[DeviceMachineType]]\n
Machine Model        : [[DeviceMachineModel]]\n
Serial Number        : [[DeviceSerialNumber]]\n
DeviceHealthStatus   : [[DeviceHealthStatus]]\n
IPv4 addresses       : [[DeviceIPV4Addresses]]\n
IPv6 addresses       : [[DeviceIPV6Addresses]]\n
Chassis              : [[DeviceChassisName]]\n
DeviceBays           : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
  Event ID         : [[EventID]]\n
  Common Event ID : [[CommonEventID]]\n
  EventSeverity    : [[EventSeverity]]\n
  Event Class      : [[EventClass]]\n
  Sequence ID      : [[EventSequenceID]]\n
  Event Source ID : [[EventSourceUUID]]\n
  Component ID     : [[EventComponentUUID]]\n
  Serial Num       : [[EventSerialNumber]]\n
  MTM              : [[EventMachineTypeModel]]\n
  EventService     : [[EventService]]\n
  Console link     : [[ConsoleLink]]\n
  iOS link         : [[iOSLink]]\n
  Android link     : [[AndroidLink]]\n
  System Name      : [[DeviceFullPathName]]\n
```

É possível clicar em **Redefinir para padrões** para alterar o formato de saída novamente para os campos padrão.

Etapa 6. Selecione **Permitir eventos excluídos** para evitar que eventos excluídos sejam encaminhados ou limpe **Permitir eventos excluídos** para encaminhar eventos excluídos. Para obter mais informações, consulte Excluindo eventos.

Etapa 7. Selecione **Habilitar este encaminhador** para ativar o encaminhamento de eventos para esse encaminhador.

Etapa 8. Clique em **Avançar** para exibir a guia **Dispositivos**.

Etapa 9. Selecione os dispositivos e os grupos que deseja monitorar para este encaminhador de evento.

Dica para encaminhar eventos para todos os dispositivos gerenciados (atuais e futuros), marque a caixa de seleção **Combinar todos os sistemas**.Se você não marcar a caixa de seleção **Combinar todos os sistemas**, certifique-se que os dispositivos selecionados não tenham um DUMMY-UUID na coluna UUID. Um Dummy-UUID é atribuído para dispositivos que ainda não se recuperaram após uma reinicialização ou não foram totalmente descobertos pelo servidor de gerenciamento. Se você selecionar um dispositivo com um Dummy-UUID, o encaminhamento de

evento funcionará para este dispositivo até o ponto quando o dispositivo for descoberto ou recuperado, e o Dummy-UUID é alterado para o UUID real.

Etapa 10. Clique em **Avançar** para exibir a guia **Eventos**.

Etapa 11. Selecione os filtros a serem usados para este encaminhador de evento.

- **Corresponder por categoria de evento**
  1. Para encaminhar todos os eventos de auditoria independentemente do nível de status, selecione **Inclui todos os eventos de Auditoria**.
  2. Para encaminhar todos os eventos de garantia, selecione **Inclui eventos de Garantia**.
  3. Para encaminhar todos os eventos de alteração de status de funcionamento, selecione **Incluir eventos de alteração de status**.
  4. Para encaminhar todos os eventos de atualização de status de funcionamento, selecione **Incluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja encaminhar.
  6. Insira os IDs para um ou mais eventos que você deseja que o encaminhamento seja excluído. Separe os IDs usando uma vírgula (por exemplo, `FQXHMEM0214I,FQXHMEM0214I`).
- **Faça a correspondência por código de evento**. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe diversos IDs usando uma vírgula.
- **Excluir por categoria de evento**.
  1. Para excluir todos os eventos de auditoria independentemente do nível de status, selecione **Excluir todos os eventos de Auditoria**.
  2. Para excluir todos os eventos de garantia, selecione **Excluir eventos de Garantia**.
  3. Para excluir todos os eventos de alteração de status de funcionamento, selecione **Excluir eventos de alteração de status**.
  4. Para excluir todos os eventos de atualização de status de funcionamento, selecione **Excluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja excluir.
  6. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe os IDs usando uma vírgula.
- **Exclua por código de evento**. Insira os IDs de um ou mais eventos que você deseja excluir. Separe diversos IDs usando uma vírgula.

Etapa 12. Decida se deve incluir determinados tipos de eventos.

- **Incluir Todos os Eventos de Auditoria**. Envia notificações sobre eventos de auditoria, com base nas classes de eventos e gravidades selecionadas.
- **Incluir eventos de Garantia**. Envia notificações sobre garantias.
- **Incluir eventos de alteração de status**. Envia notificações sobre alterações no status.
- **Incluir eventos de atualização de status**. Enviou notificações sobre novos alertas
- **Incluir eventos do boletim**. Envia notificação sobre novos boletins.

Etapa 13. Selecione os tipos de eventos e as gravidades sobre os quais deseja ser notificado.

Etapa 14. Selecione se deve filtrar eventos por capacidade de manutenção.

Etapa 15. Clique em **Avançar** para exibir a guia **Planejador**.

Etapa 16. **Opcional:** Defina a hora e os dias em que deseja que os eventos especificados sejam encaminhados para este encaminhador de evento. Apenas eventos que ocorrem durante o slot de tempo especificado são encaminhados.

Se você não criar um planejamento para o encaminhador de evento, os eventos serão encaminhados 24h por dia/7 dias por semana.

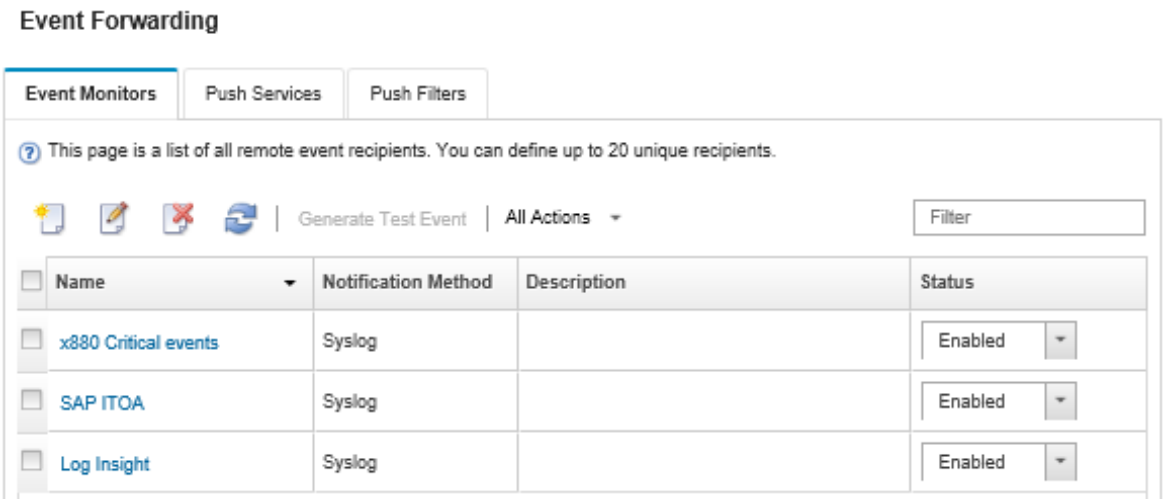
1. Use o ícone **Rolar para a esquerda** (◀) e o ícone **Rolar para a direita** (▶), e os botões **Dia**, **Semana** e **Mês** para localizar o dia e a hora em que você deseja iniciar o planejamento.

2. Clique duas vezes no slot de tempo para abrir a caixa de diálogo Novo Período de Tempo.
3. Preencha as informações necessárias, incluindo a data e a hora de início e encerramento, e se está planejado para ocorrer novamente.
4. Clique em **Criar** para salvar o planejamento e fechar a caixa de diálogo. O novo planejamento é incluído no calendário.

Dica:
- É possível alterar o período arrastando a entrada de programação para outro período no calendário.
- É possível alterar a duração selecionando o início ou o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar o horário de encerramento selecionando o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar uma programação clicando duas vezes na entrada da programação no calendário e clicando em **Editar Entrada**.
- É possível exibir um resumo de todas as entradas da programação selecionando **Mostrar Resumo do Planejador**. O resumo inclui o período de cada entrada e quais entradas são repetíveis.
- É possível excluir uma entrada da programação do calendário ou do resumo planejador selecionando a entrada e clicando em **Excluir Entrada**.

Etapa 17. Clique em **Criar**.

O encaminhador de evento está listado na tabela Encaminhamento de Evento.



Etapa 18. Selecione o novo encaminhador de evento, clique em **Gerar Evento de Teste** e verifique se os eventos foram encaminhados corretamente para o serviço de e-mail apropriado.

Depois de concluir

Na página Encaminhamento de Evento, é possível executar as seguintes ações em um encaminhador de evento selecionado:

- Atualizar a lista de encaminhadores de evento clicando no ícone **Atualizar** ( ).
- Exibir detalhes sobre um encaminhador de evento específico, clicando no link na coluna **Nome**.
- Alterar as propriedades do encaminhador de evento e filtrar os critérios clicando no nome do encaminhador de evento na coluna **Nome**.
- Excluir o encaminhador de evento clicando no ícone **Excluir** ( ).

- Suspender o encaminhamento de evento (consulte Suspendendo o encaminhamento de evento).

Configurando o encaminhamento de evento em um serviço SMTP do Gmail

É possível configurar o Lenovo XClarity Administrator para encaminhar eventos monitorados para um serviço de e-mail baseado na web, como Gmail.

Use os seguintes exemplos de configuração para ajudá-lo a configurar seu encaminhador de evento para usar o serviço Gmail SMTP.

Nota: Gmail recomenda o usar o método de autenticação OAUTH2 para comunicação mais seguro. Se você optar por usar autenticação regular, você receberá um e-mail indicando que um aplicativo tentou usar sua conta sem usar os padrões de segurança mais recente. O e-mail inclui instruções para configurar sua conta de e-mail para aceitar esses tipos de aplicativos.

Para obter informações sobre como configurar um servidor SMTP Gmail, consulte https://support.google.com/a/answer/176600?hl=en.

Autenticação normal usando SSL na porta 465

Este exemplo comunica-se com o servidor SMTP Gmail usando o protocolo SSL na porta 465 e autentica-o usando uma conta de usuário e senha do Gmail válidos.

Parâmetro	Valor
Host	smtp.gmail.com
Porta	465
SSL	Selecionar
STARTTLS	Limpar
Autenticação	Regular
Usuário	Endereço de e-mail do Gmail válido
Senha	Senha de autenticação do Gmail
Do endereço	(opcional)

Autenticação normal usando TLS na porta 587

Este exemplo comunica-se com o servidor SMTP Gmail usando o protocolo TLS na porta 587 e autentica-o usando uma conta de usuário e senha do Gmail válidos.

Parâmetro	Valor
Host	smtp.gmail.com
Porta	587
SSL	Limpar
STARTTLS	Selecionar
Autenticação	Regular
Usuário	Endereço de e-mail do Gmail válido
Senha	Senha de autenticação do Gmail
Do endereço	(opcional)

Autenticação OAUTH2 usando TLS na porta 587

Este exemplo comunica-se com o servidor SMTP Gmail usando o protocolo TLS na porta 587 e autentica-o usando uma conta de usuário e token de segurança do Gmail válidos.

Use o seguinte procedimento de amostra para obter o token de segurança.

1. Crie um projeto no Console dos Desenvolvedores do Google e recupere o ID e o segredo do cliente. Para obter mais informações, consulte o website Página Google Sign-In for Websites.
   a. Em um navegador da Web, abra o Página Google APIs.
   b. Clique em **Selecione um projeto → Crie um projeto** no menu nesta página da Web. A caixa de diálogo Novo Projeto é exibida.
   c. Digite um nome, selecione **Sim** para concordar o contrato de licença e clique em **Criar**.
   d. Na guia **Visão Geral**, use o campo de pesquisa para procurar por "Gmail."
   e. Clique em **API DO GMAIL** nos resultados da pesquisa.
   f. Clique em **Habilitar**.
   g. Clique na guia **Credenciais do Usuário**.
   h. Clique em **Tela do acordo de OAuth**.
   i. Digite um nome no campo **Nome do produto mostrado aos usuários** e clique em **Salvar**.
   j. Clique em **Criar credenciais → ID do cliente OAuth**.
   k. Selecione **Outro** e insira um nome.
   l. Clique em **Criar**. A caixa de diálogo OAuth client é exibida com seu ID do cliente e cliente em segredo.
   m. Registre o ID do e o segredo do cliente para uso posterior.
   n. Clique em **OK** para fechar a caixa de diálogo.
2. Use o script do Python oauth2.py para gerar e autorizar um token de segurança, inserindo o ID e o segredo do cliente que foi gerado quando você criou o projeto.

   Nota: O Python 2.7 é necessário para concluir esta etapa. É possível baixar e instalar o Python 2.7 a partir do Site do Python).
   a. Em um navegador da Web, abra o Página gmail-oauth2-tools.
   b. Clique em **Bruto** e, em seguida, salve o conteúdo como um nome de arquivo `oauth2.py` no sistema local.
   c. Execute o seguinte comando no terminal (Linux) ou uma linha de comandos (Windows):

```
py oauth2.py --user=<your_email> --client_id=<client_id>
   --client_secret=<client_secret> --generate_oauth2_token
```

   Exemplo

```
py oauth2.py --user=jon@gmail.com
   --client_id=884243132302-458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com
   --client_secret=3tnyXgEiBIbT2mOOzqnlTszk --generate_oauth2_token
```

   Esse comando retorna uma URL que você deve usar para autorizar o token e para recuperar um código de verificação do website do Google, por exemplo:

```
To authorize token, visit this url and follow the directions:

https://accounts.google.com/o/oauth2/auth?client_id=884243132302
-458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com&amp;redirect_uri=
urn%3Aietf%3Awg%3Aoauth%3A2.0%3Aoob&amp;response_type=code&amp;scope=https%3A%2F%2Fmail.
google.com%2F
```

```
Enter verification code:
```

d. Em um navegador da Web, abra a URL que foi retornada na etapa anterior.

e. Clique em **Permitir** para concordar com este serviço. Um código de verificação a ser retornado.

f. Insira o código de verificação no comando `oauth2.py`.

O comando retorna o token de segurança e atualiza o token, por exemplo:

```
Refresh Token: 1/K8lPGx6UQQajj7tQGYKq8mVG8lVvGIVzHqzxFIMeYEQMEudVrK5jSpoR3OzcRFq6
Access Token: ya29.CjHXAsyoH9GuCZutgIOxm1SGSqKrUkjIoH14SGMnljZ6rwp3gZmK7SrGDPCQx_KN-34f
Access Token Expiration Seconds: 3600
```

Importante: O token de segurança expira após um período de tempo. Você pode usar o script do Python oauth2.py e o token atualizado para gerar um novo token de segurança. É sua responsabilidade gerar um novo token de segurança e o atualizar o encaminhador de evento no Lenovo XClarity Administrator com o novo token.

3. Na interface da Web Lenovo XClarity Administrator, configure o encaminhador de evento por e-mail usando os seguintes atributos:

Parâmetro	Valor
Host	smtp.gmail.com
Porta	587
SSL	Limpar
STARTTLS	Selecionar
Autenticação	OAUTH2
Usuário	Endereço de e-mail do Gmail válido
Token	Token de segurança
Do endereço	(opcional)

Configurando o encaminhamento de evento em um servidor FTP

É possível configurar o Lenovo XClarity Administrator para encaminhar eventos específicos a um servidor FTP.

Sobre esta tarefa

É possível criar e habilitar até 20 encaminhadores de evento para enviar eventos a destinatários específicos.

Se o XClarity Administrator for reinicializado após os encaminhadores de evento serem configurados, você deverá aguardar o servidor de gerenciamento para gerar novamente dados internos antes que os eventos sejam encaminhados corretamente.

Nota: Para XClarity Administrator v1.2.0 e posterior, os **Comutadores** são incluído na guia **Eventos** nas caixas de diálogo Novo Encaminhador de Eventos e Alterar Encaminhador de Eventos. Se você atualizou para 1.2.0 ou posterior de uma versão anterior, lembre-se de atualizar seus encaminhadores de evento para incluir ou excluir os eventos de RackSwitch conforme apropriado. Isso será necessário mesmo se você tiver marcado a caixa de seleção **Todos os Sistemas** para selecionar todos os dispositivos.

Procedimento

Conclua as etapas a seguir para criar um encaminhador de evento para um servidor FTP.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Encaminhamento de Evento**. A página Encaminhamento de Evento é exibida.

Etapa 2. Clique na guia **Encaminhamento de eventos**.

Etapa 3. Clique no ícone **Criar** ( ). A guia **Geral** da caixa de diálogo Novo Encaminhador de Evento é exibida.

Etapa 4. Selecione **FTP** como o tipo de encaminhador de evento e preencha as informações específicas do protocolo:

- Digite o nome, o host de destino e a descrição opcional para os encaminhadores do evento.
- Insira a porta a ser usada para o encaminhamento de eventos. O padrão é 21.
- Insira o período de tempo limite (em segundos) para a solicitação. O padrão é 30 segundos.
- **Opcional:** especificar a sequência de caracteres a ser removido do conteúdo do arquivo.
- Insira o formato do nome do arquivo a ser usado pelo arquivo que contém o evento encaminhado. O formato padrão é `event_[[EventSequenceID]].txt`.

  Nota: Cada arquivo contém informações para um único evento.
- Insira o caminho no servidor FTP remoto onde o arquivo deve ser carregado.
- Escolha a codificação de caracteres **UTF 8** ou **Big5**. O padrão é UTF-8.
- Selecione o tipo de autenticação. Este pode ser um dos valores a seguir.
  - **Anônimo**. (padrão) Nenhuma autenticação é usada
  - **Básico**. Autentica ao servidor FTP usando o ID e senha do usuário especificado.

Etapa 5. Clique em **Formato de saída** para escolher o formato de saída dos dados de evento a serem encaminhados. As informações variam para cada tipo de encaminhadores de evento.

O formato de saída de exemplo a seguir é o formato padrão para destinatários do FTP. Todas as palavras entre colchetes duplos são as variáveis que são substituídas por valores reais quando um evento é encaminhado. As variáveis disponíveis para destinatários do FTP estão listadas na caixa de diálogo Formato de Saída.

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name          : [[DeviceName]]\n
Product name         : [[DeviceProductName]]\n
Host name            : [[DeviceHostName]]\n
Machine Type         : [[DeviceMachineType]]\n
Machine Model        : [[DeviceMachineModel]]\n
Serial Number        : [[DeviceSerialNumber]]\n
DeviceHealthStatus   : [[DeviceHealthStatus]]\n
IPv4 addresses       : [[DeviceIPV4Addresses]]\n
IPv6 addresses       : [[DeviceIPV6Addresses]]\n
Chassis              : [[DeviceChassisName]]\n
DeviceBays           : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
  Event ID         : [[EventID]]\n
  Common Event ID : [[CommonEventID]]\n
  EventSeverity    : [[EventSeverity]]\n
  Event Class      : [[EventClass]]\n
  Sequence ID      : [[EventSequenceID]]\n
  Event Source ID : [[EventSourceUUID]]\n
```

```
Component ID    : [[EventComponentUUID]]\n
Serial Num      : [[EventSerialNumber]]\n
MTM             : [[EventMachineTypeModel]]\n
EventService    : [[EventService]]\n
Console link    : [[ConsoleLink]]\n
iOS link        : [[iOSLink]]\n
Android link    : [[AndroidLink]]\n
System Name     : [[DeviceFullPathName]]\n"
```

É possível clicar em **Redefinir para padrões** para alterar o formato de saída novamente para os campos padrão.

Etapa 6. Selecione **Permitir eventos excluídos** para evitar que eventos excluídos sejam encaminhados ou limpe **Permitir eventos excluídos** para encaminhar eventos excluídos. Para obter mais informações, consulte Excluindo eventos.

Etapa 7. Selecione **Habilitar este encaminhador** para ativar o encaminhamento de eventos para esse encaminhador.

Etapa 8. Clique em **Avançar** para exibir a guia **Dispositivos**.

Etapa 9. Selecione os dispositivos e os grupos que deseja monitorar para este encaminhador de evento.

Dica para encaminhar eventos para todos os dispositivos gerenciados (atuais e futuros), marque a caixa de seleção **Combinar todos os sistemas**.Se você não marcar a caixa de seleção **Combinar todos os sistemas**, certifique-se que os dispositivos selecionados não tenham um DUMMY-UUID na coluna UUID. Um Dummy-UUID é atribuído para dispositivos que ainda não se recuperaram após uma reinicialização ou não foram totalmente descobertos pelo servidor de gerenciamento. Se você selecionar um dispositivo com um Dummy-UUID, o encaminhamento de evento funcionará para este dispositivo até o ponto quando o dispositivo for descoberto ou recuperado, e o Dummy-UUID é alterado para o UUID real.

Etapa 10. Clique em **Avançar** para exibir a guia **Eventos**.

Etapa 11. Selecione os filtros a serem usados para este encaminhador de evento.

- **Corresponder por categoria de evento**
  1. Para encaminhar todos os eventos de auditoria independentemente do nível de status, selecione **Inclui todos os eventos de Auditoria**.
  2. Para encaminhar todos os eventos de garantia, selecione **Inclui eventos de Garantia**.
  3. Para encaminhar todos os eventos de alteração de status de funcionamento, selecione **Incluir eventos de alteração de status**.
  4. Para encaminhar todos os eventos de atualização de status de funcionamento, selecione **Incluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja encaminhar.
  6. Insira os IDs para um ou mais eventos que você deseja que o encaminhamento seja excluído. Separe os IDs usando uma vírgula (por exemplo, `FQXHMEM0214I`,`FQXHMEM0214I`).
- **Faça a correspondência por código de evento**. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe diversos IDs usando uma vírgula.
- **Excluir por categoria de evento**.
  1. Para excluir todos os eventos de auditoria independentemente do nível de status, selecione **Excluir todos os eventos de Auditoria**.
  2. Para excluir todos os eventos de garantia, selecione **Excluir eventos de Garantia**.
  3. Para excluir todos os eventos de alteração de status de funcionamento, selecione **Excluir eventos de alteração de status**.
  4. Para excluir todos os eventos de atualização de status de funcionamento, selecione **Excluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja excluir.

6. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe os IDs usando uma vírgula.

- **Exclua por código de evento**. Insira os IDs de um ou mais eventos que você deseja excluir. Separe diversos IDs usando uma vírgula.

Etapa 12. Decida se deve incluir determinados tipos de eventos.
- **Incluir Todos os Eventos de Auditoria**. Envia notificações sobre eventos de auditoria, com base nas classes de eventos e gravidades selecionadas.
- **Incluir eventos de Garantia**. Envia notificações sobre garantias.
- **Incluir eventos de alteração de status**. Envia notificações sobre alterações no status.
- **Incluir eventos de atualização de status**. Enviou notificações sobre novos alertas
- **Incluir eventos do boletim**. Envia notificação sobre novos boletins.

Etapa 13. Selecione os tipos de eventos e as gravidades sobre os quais deseja ser notificado.

Etapa 14. Selecione se deve filtrar eventos por capacidade de manutenção.

Etapa 15. Clique em **Avançar** para exibir a guia **Planejador**.

Etapa 16. **Opcional:** Defina a hora e os dias em que deseja que os eventos especificados sejam encaminhados para este encaminhador de evento. Apenas eventos que ocorrem durante o slot de tempo especificado são encaminhados.

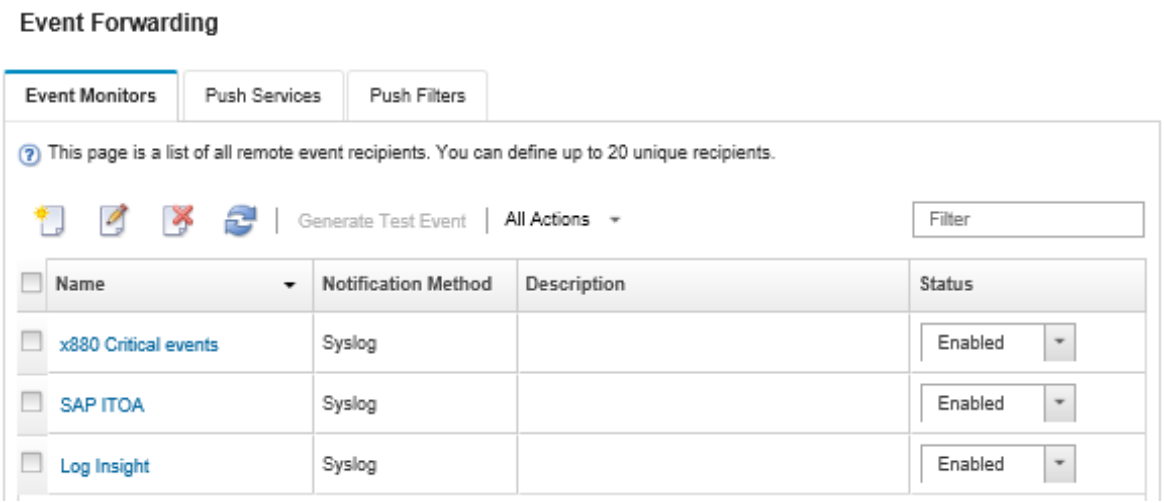
Se você não criar um planejamento para o encaminhador de evento, os eventos serão encaminhados 24h por dia/7 dias por semana.

1. Use o ícone **Rolar para a esquerda** (◀) e o ícone **Rolar para a direita** (▶), e os botões **Dia**, **Semana** e **Mês** para localizar o dia e a hora em que você deseja iniciar o planejamento.
2. Clique duas vezes no slot de tempo para abrir a caixa de diálogo Novo Período de Tempo.
3. Preencha as informações necessárias, incluindo a data e a hora de início e encerramento, e se está planejado para ocorrer novamente.
4. Clique em **Criar** para salvar o planejamento e fechar a caixa de diálogo. O novo planejamento é incluído no calendário.

Dica:
- É possível alterar o período arrastando a entrada de programação para outro período no calendário.
- É possível alterar a duração selecionando o início ou o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar o horário de encerramento selecionando o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar uma programação clicando duas vezes na entrada da programação no calendário e clicando em **Editar Entrada**.
- É possível exibir um resumo de todas as entradas da programação selecionando **Mostrar Resumo do Planejador**. O resumo inclui o período de cada entrada e quais entradas são repetíveis.
- É possível excluir uma entrada da programação do calendário ou do resumo planejador selecionando a entrada e clicando em **Excluir Entrada**.

Etapa 17. Clique em **Criar**.

O encaminhador de evento está listado na tabela Encaminhamento de Evento.



Etapa 18. Selecione o novo encaminhador de evento, clique em **Gerar Evento de Teste** e verifique se os eventos foram encaminhados corretamente para o servidor FTP apropriado.

Depois de concluir

Na página Encaminhamento de Evento, é possível executar as seguintes ações em um encaminhador de evento selecionado:

- Atualizar a lista de encaminhadores de evento clicando no ícone **Atualizar** ( ).
- Exibir detalhes sobre um encaminhador de evento específico, clicando no link na coluna **Nome**.
- Alterar as propriedades do encaminhador de evento e filtrar os critérios clicando no nome do encaminhador de evento na coluna **Nome**.
- Excluir o encaminhador de evento clicando no ícone **Excluir** ( ).
- Suspender o encaminhamento de evento (consulte Suspendendo o encaminhamento de evento).

Configurando o encaminhamento de evento em um serviço Web REST

É possível configurar o Lenovo XClarity Administrator para encaminhar eventos específicos a um serviço da Web REST.

Sobre esta tarefa

É possível criar e habilitar até 20 encaminhadores de evento para enviar eventos a destinatários específicos.

Se o XClarity Administrator for reinicializado após os encaminhadores de evento serem configurados, você deverá aguardar o servidor de gerenciamento para gerar novamente dados internos antes que os eventos sejam encaminhados corretamente.

Nota: Para XClarity Administrator v1.2.0 e posterior, os **Comutadores** são incluído na guia **Eventos** nas caixas de diálogo Novo Encaminhador de Eventos e Alterar Encaminhador de Eventos. Se você atualizou para 1.2.0 ou posterior de uma versão anterior, lembre-se de atualizar seus encaminhadores de evento para incluir ou excluir os eventos de RackSwitch conforme apropriado. Isso será necessário mesmo se você tiver marcado a caixa de seleção **Todos os Sistemas** para selecionar todos os dispositivos.

Procedimento

Conclua as etapas a seguir para criar um encaminhador de evento para um serviço Web REST.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Encaminhamento de Evento**. A página Encaminhamento de Evento é exibida.

Etapa 2. Clique na guia **Encaminhamento de eventos**.

Etapa 3. Clique no ícone **Criar** ( ). A guia **Geral** da caixa de diálogo Novo Encaminhador de Evento é exibida.

Etapa 4. Selecione **REST** como o tipo de encaminhador de evento e preencha as informações específicas do protocolo:

- Insira o caminho do recurso em que o encaminhador deve publicar os eventos (por exemplo, /rest/test).
- Selecione o protocolo a ser usado para o encaminhamento de eventos. Este pode ser um dos valores a seguir.
  - **HTTP**
  - **HTTPS**
- Selecione o método REST. Este pode ser um dos valores a seguir.
  - **PUT**
  - **POST**
- Insira o período de tempo limite (em segundos) para a solicitação. O padrão é 30 segundos.
- **Opcional:** Se a autenticação for necessária, selecione um dos tipos de autenticação a seguir:
  - **Básico**. Autentica ao servidor especificado usando o ID do usuário e senha especificados.
  - **Nenhum**. Nenhuma autenticação é usada.

Etapa 5. Clique em **Formato de saída** para escolher o formato de saída dos dados de evento a serem encaminhados. As informações variam para cada tipo de encaminhador de evento.

O formato de saída de exemplo a seguir é o formato padrão para destinatários do serviço Web REST. Todas as palavras entre colchetes duplos são as variáveis que são substituídas por valores reais quando um evento é encaminhado. As variáveis disponíveis para destinatários do serviço Web REST estão listadas na caixa de diálogo Formato de Saída.

```
{\"msg\":\"[[EventMessage]]\",\"eventID\":\"[[EventID]]\",\"serialnum\":
\"[[EventSerialNumber]]\",\"senderUUID\":\"[[EventSenderUUID]]\",\"flags\":
\"[[EventFlags]]\",\"userid\":\"[[EventUserName]]\",\"localLogID\":
\"[[EventLocalLogID]]\",\"systemName\":\"[[DeviceFullPathName]]\",\"action\":
[[EventActionNumber]],\"failFRUNumbers\":\"[[EventFailFRUs]]\",\"severity\":
[[EventSeverityNumber]],\"sourceID\":\"[[EventSourceUUID]]\",
\"sourceLogSequence\":[[EventSourceLogSequenceNumber]],\"failFRUSNs\":
\"[[EventFailSerialNumbers]]\",\"failFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",
\"eventClass\":[[EventClassNumber]],\"componentID\":\"[[EventComponentUUID]]\",
\"mtm\":\"[[EventMachineTypeModel]]\",\"msgID\":\"[[EventMessageID]]\",
"sequenceNumber\":\"[[EventSequenceID]]\",\"timeStamp\":\"[[EventTimeStamp]]\",
\"args\":[[EventMessageArguments]],\"service\":[[EventServiceNumber]],
\"commonEventID\":\"[[CommonEventID]]\",\"eventDate\":\"[[EventDate]]\"}"
```

É possível clicar em **Redefinir para padrões** para alterar o formato de saída novamente para os campos padrão.

Etapa 6. Selecione **Permitir eventos excluídos** para evitar que eventos excluídos sejam encaminhados ou limpe **Permitir eventos excluídos** para encaminhar eventos excluídos. Para obter mais informações, consulte Excluindo eventos.

Etapa 7. Selecione **Habilitar este encaminhador** para ativar o encaminhamento de eventos para esse encaminhador.

Etapa 8. Clique em **Avançar** para exibir a guia **Dispositivos**.

Etapa 9. Selecione os dispositivos e os grupos que deseja monitorar para este encaminhador de evento.

Dica para encaminhar eventos para todos os dispositivos gerenciados (atuais e futuros), marque a caixa de seleção **Combinar todos os sistemas**.Se você não marcar a caixa de seleção **Combinar todos os sistemas**, certifique-se que os dispositivos selecionados não tenham um DUMMY-UUID na coluna UUID. Um Dummy-UUID é atribuído para dispositivos que ainda não se recuperaram após uma reinicialização ou não foram totalmente descobertos pelo servidor de gerenciamento. Se você selecionar um dispositivo com um Dummy-UUID, o encaminhamento de evento funcionará para este dispositivo até o ponto quando o dispositivo for descoberto ou recuperado, e o Dummy-UUID é alterado para o UUID real.

Etapa 10. Clique em **Avançar** para exibir a guia **Eventos**.

Etapa 11. Selecione os filtros a serem usados para este encaminhador de evento.

- **Corresponder por categoria de evento**
  1. Para encaminhar todos os eventos de auditoria independentemente do nível de status, selecione **Inclui todos os eventos de Auditoria**.
  2. Para encaminhar todos os eventos de garantia, selecione **Inclui eventos de Garantia**.
  3. Para encaminhar todos os eventos de alteração de status de funcionamento, selecione **Incluir eventos de alteração de status**.
  4. Para encaminhar todos os eventos de atualização de status de funcionamento, selecione **Incluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja encaminhar.
  6. Insira os IDs para um ou mais eventos que você deseja que o encaminhamento seja excluído. Separe os IDs usando uma vírgula (por exemplo, `FQXHMEM0214I`,`FQXHMEM0214I`).
- **Faça a correspondência por código de evento**. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe diversos IDs usando uma vírgula.
- **Excluir por categoria de evento**.
  1. Para excluir todos os eventos de auditoria independentemente do nível de status, selecione **Excluir todos os eventos de Auditoria**.
  2. Para excluir todos os eventos de garantia, selecione **Excluir eventos de Garantia**.
  3. Para excluir todos os eventos de alteração de status de funcionamento, selecione **Excluir eventos de alteração de status**.
  4. Para excluir todos os eventos de atualização de status de funcionamento, selecione **Excluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja excluir.
  6. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe os IDs usando uma vírgula.
- **Exclua por código de evento**. Insira os IDs de um ou mais eventos que você deseja excluir. Separe diversos IDs usando uma vírgula.

Etapa 12. Decida se deve incluir determinados tipos de eventos.

- **Incluir Todos os Eventos de Auditoria**. Envia notificações sobre eventos de auditoria, com base nas classes de eventos e gravidades selecionadas.
- **Incluir eventos de Garantia**. Envia notificações sobre garantias.
- **Incluir eventos de alteração de status**. Envia notificações sobre alterações no status.
- **Incluir eventos de atualização de status**. Enviou notificações sobre novos alertas
- **Incluir eventos do boletim**. Envia notificação sobre novos boletins.

Etapa 13. Selecione os tipos de eventos e as gravidades sobre os quais deseja ser notificado.

Etapa 14. Selecione se deve filtrar eventos por capacidade de manutenção.

Etapa 15. Clique em **Avançar** para exibir a guia **Planejador**.

Etapa 16. **Opcional:** Defina a hora e os dias em que deseja que os eventos especificados sejam encaminhados para este encaminhador de evento. Apenas eventos que ocorrem durante o slot de tempo especificado são encaminhados.

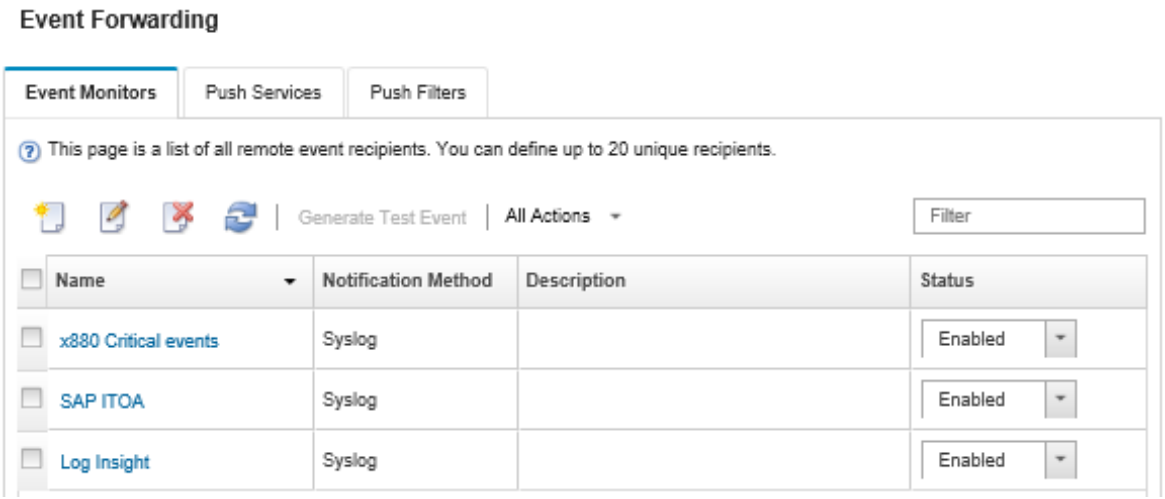
Se você não criar um planejamento para o encaminhador de evento, os eventos serão encaminhados 24h por dia/7 dias por semana.

1. Use o ícone **Rolar para a esquerda** (◀) e o ícone **Rolar para a direita** (▶), e os botões **Dia**, **Semana** e **Mês** para localizar o dia e a hora em que você deseja iniciar o planejamento.
2. Clique duas vezes no slot de tempo para abrir a caixa de diálogo Novo Período de Tempo.
3. Preencha as informações necessárias, incluindo a data e a hora de início e encerramento, e se está planejado para ocorrer novamente.
4. Clique em **Criar** para salvar o planejamento e fechar a caixa de diálogo. O novo planejamento é incluído no calendário.

Dica:
- É possível alterar o período arrastando a entrada de programação para outro período no calendário.
- É possível alterar a duração selecionando o início ou o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar o horário de encerramento selecionando o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar uma programação clicando duas vezes na entrada da programação no calendário e clicando em **Editar Entrada**.
- É possível exibir um resumo de todas as entradas da programação selecionando **Mostrar Resumo do Planejador**. O resumo inclui o período de cada entrada e quais entradas são repetíveis.
- É possível excluir uma entrada da programação do calendário ou do resumo planejador selecionando a entrada e clicando em **Excluir Entrada**.

Etapa 17. Clique em **Criar**.

O encaminhador de evento está listado na tabela Encaminhamento de Evento.



Etapa 18. Selecione o novo encaminhador de evento, clique em **Gerar Evento de Teste** e verifique se os eventos foram encaminhados corretamente para o serviço Web REST apropriado.

Depois de concluir

Na página Encaminhamento de Evento, é possível executar as seguintes ações em um encaminhador de evento selecionado:

- Atualizar a lista de encaminhadores de evento clicando no ícone **Atualizar** ( ).
- Exibir detalhes sobre um encaminhador de evento específico, clicando no link na coluna **Nome**.
- Alterar as propriedades do encaminhador de evento e filtrar os critérios clicando no nome do encaminhador de evento na coluna **Nome**.
- Excluir o encaminhador de evento clicando no ícone **Excluir** ( ).
- Suspender o encaminhamento de evento (consulte Suspendendo o encaminhamento de evento).

Configurando o encaminhamento de eventos para um gerenciador remoto de SNMPv1 ou de SNMPv3

É possível configurar o Lenovo XClarity Administrator para encaminhar eventos específicos para um gerenciador remoto de SNMPv1 ou de SNMPv3.

Sobre esta tarefa

É possível criar e habilitar até 20 encaminhadores de evento para enviar eventos a destinatários específicos.

Se o XClarity Administrator for reinicializado após os encaminhadores de evento serem configurados, você deverá aguardar o servidor de gerenciamento para gerar novamente dados internos antes que os eventos sejam encaminhados corretamente.

Nota: Para XClarity Administrator v1.2.0 e posterior, os **Comutadores** são incluído na guia **Eventos** nas caixas de diálogo Novo Encaminhador de Eventos e Alterar Encaminhador de Eventos. Se você atualizou para 1.2.0 ou posterior de uma versão anterior, lembre-se de atualizar seus encaminhadores de evento para incluir ou excluir os eventos de RackSwitch conforme apropriado. Isso será necessário mesmo se você tiver marcado a caixa de seleção **Todos os Sistemas** para selecionar todos os dispositivos.

Para obter informações sobre o XClarity Administrator MIB, consulte arquivo lenovoMgrAlert.mib.

Procedimento

Conclua as seguintes etapas para criar um encaminhador de evento para um gerenciador remoto de SNMPv1 ou de SNMPv3.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Encaminhamento de Evento**. A página Encaminhamento de Evento é exibida.

Etapa 2. Clique na guia **Encaminhamento de eventos**.

Etapa 3. Clique no ícone **Criar** ( ). A guia **Geral** da caixa de diálogo Novo Encaminhador de Evento é exibida.

Etapa 4. Selecione **SNMPv1** ou **SNMPv3** como o tipo de encaminhador de evento e preencha as informações específicas do protocolo:

- Digite o nome e o host de destino para o encaminhador do evento.
- Insira a porta a ser usada para o encaminhamento de eventos. O padrão é `162`.
- **Opcional:** insira informações adicionais, incluindo a descrição, nome de contato e local.
- Selecione a versão do SNMP. Este pode ser um dos valores a seguir.
  - **SNMPv1**. Se essa versão estiver selecionada, especifique a senha da comunidade enviada com cada solicitação de SNMP ao dispositivo.

– **SNMPv3**. Esta é a versão padrão e é recomendada para segurança aprimorada. Se SNMPv3 estiver selecionado, opcionalmente, especifique o ID do usuário, o tipo de autenticação e senha, e o tipo e senha de privacidade.

  Se o receptor do trap SNMPv3 precisar do ID do mecanismo para a instância do XClarity Administrator, é possível localizá-lo executando as seguintes etapas:

  1. Certifique-se de que os parâmetros de conexão (nome de usuário, authProtocol, authPassword, privProtocol, privPassword) correspondam aos parâmetros configurados em XClarity Administrator.
  2. Usando o software preferencial (como o snmpwalk), execute uma solicitação GET do SNMP no servidor do XClarity Administrator usando um dos OIDs a seguir:
     – EngineID: 1.3.6.1.6.3.10.2.1.1.0
     – EngineBoots: 1.3.6.1.6.3.10.2.1.2.0

     Use a seguinte sintaxe para o comando `snmpget`. Observe que o tipo de autenticação do encaminhador pode ser SHA ou em branco (sem autenticação).
     ```
     snmpget -v 3 -u <FORWARDER_USER_ID> -l authPriv -a <FORWARDER_AUTH_TYPE> -A <FORWARDE
     ```

     Por exemplo, se o endereço IP do XClarity Administrator for 192.0.1.0, o tipo de autenticação for SHA e o tipo de privacidade for AES, o comando a seguir exibirá o engineID.
     ```
     snmpget -v 3 -u someUserID -l authPriv -a SHA -A someUserIDPassword_1 -x AES -X somePrivacyPassword_
     ```

     A resposta de exemplo a seguir é retornada. Neste exemplo, o engineID é 0x80001370017F00000134C27E12.
     ```
     iso.3.6.1.6.3.10.2.1.1.0 = Hex-STRING: 80 00 13 70 01 7F 00 00 01 34 C2 7E 12
     ```

- Insira o período de tempo limite (em segundos) para a solicitação. O padrão é 30 segundos.
- **Opcional**: se a autenticação do trap for necessária, insira o ID do usuário e a senha de autenticação. O mesmo ID do usuário e a mesma senha devem ser inseridos no gerenciador de SNMP remoto para o qual os traps são encaminhados.
- Selecione o protocolo de autenticação usado pelo gerenciador de SNMP remoto para verificar o remetente do trap. Este pode ser um dos valores a seguir
  – **SHA**. Usa o protocolo SHA para autenticação ao servidor SNMP especificado usando o ID do usuário, senha e nome de domínio especificados.
  – **Nenhum**. Nenhuma autenticação é usada
- Se a criptografia do trap for necessária, insira o tipo de privacidade (protocolo de criptografia) e a senha. Este pode ser um dos valores a seguir. O mesmo protocolo e a mesma senha devem ser inseridos no gerenciador de SNMP remoto para o qual os traps são encaminhados.
  – **AES**
  – **DES**
  – **Nenhum**

Etapa 5. Selecione **Permitir eventos excluídos** para evitar que eventos excluídos sejam encaminhados ou limpe **Permitir eventos excluídos** para encaminhar eventos excluídos. Para obter mais informações, consulte Excluindo eventos.

Etapa 6. Selecione **Habilitar este encaminhador** para ativar o encaminhamento de eventos para esse encaminhador.

Etapa 7. Clique em **Avançar** para exibir a guia **Dispositivos**.

Etapa 8. Selecione os dispositivos e os grupos que deseja monitorar para este encaminhador de evento.

Dica para encaminhar eventos para todos os dispositivos gerenciados (atuais e futuros), marque a caixa de seleção **Combinar todos os sistemas**.Se você não marcar a caixa de seleção **Combinar todos os sistemas**, certifique-se que os dispositivos selecionados não tenham um DUMMY-UUID na coluna UUID. Um Dummy-UUID é atribuído para dispositivos que ainda não se

recuperaram após uma reinicialização ou não foram totalmente descobertos pelo servidor de gerenciamento. Se você selecionar um dispositivo com um Dummy-UUID, o encaminhamento de evento funcionará para este dispositivo até o ponto quando o dispositivo for descoberto ou recuperado, e o Dummy-UUID é alterado para o UUID real.

Etapa 9. Clique em **Avançar** para exibir a guia **Eventos**.

Etapa 10. Selecione os filtros a serem usados para este encaminhador de evento.

- **Corresponder por categoria de evento**
  1. Para encaminhar todos os eventos de auditoria independentemente do nível de status, selecione **Inclui todos os eventos de Auditoria**.
  2. Para encaminhar todos os eventos de garantia, selecione **Inclui eventos de Garantia**.
  3. Para encaminhar todos os eventos de alteração de status de funcionamento, selecione **Incluir eventos de alteração de status**.
  4. Para encaminhar todos os eventos de atualização de status de funcionamento, selecione **Incluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja encaminhar.
  6. Insira os IDs para um ou mais eventos que você deseja que o encaminhamento seja excluído. Separe os IDs usando uma vírgula (por exemplo, `FQXHMEM0214I,FQXHMEM0214I`).
- **Faça a correspondência por código de evento**. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe diversos IDs usando uma vírgula.
- **Excluir por categoria de evento**.
  1. Para excluir todos os eventos de auditoria independentemente do nível de status, selecione **Excluir todos os eventos de Auditoria**.
  2. Para excluir todos os eventos de garantia, selecione **Excluir eventos de Garantia**.
  3. Para excluir todos os eventos de alteração de status de funcionamento, selecione **Excluir eventos de alteração de status**.
  4. Para excluir todos os eventos de atualização de status de funcionamento, selecione **Excluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja excluir.
  6. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe os IDs usando uma vírgula.
- **Exclua por código de evento**. Insira os IDs de um ou mais eventos que você deseja excluir. Separe diversos IDs usando uma vírgula.

Etapa 11. Decida se deve incluir determinados tipos de eventos.

- **Incluir Todos os Eventos de Auditoria**. Envia notificações sobre eventos de auditoria, com base nas classes de eventos e gravidades selecionadas.
- **Incluir eventos de Garantia**. Envia notificações sobre garantias.
- **Incluir eventos de alteração de status**. Envia notificações sobre alterações no status.
- **Incluir eventos de atualização de status**. Enviou notificações sobre novos alertas
- **Incluir eventos do boletim**. Envia notificação sobre novos boletins.

Etapa 12. Selecione os tipos de eventos e as gravidades sobre os quais deseja ser notificado.

Etapa 13. Selecione se deve filtrar eventos por capacidade de manutenção.

Etapa 14. Clique em **Avançar** para exibir a guia **Planejador**.

Etapa 15. **Opcional:** Defina a hora e os dias em que deseja que os eventos especificados sejam encaminhados para este encaminhador de evento. Apenas eventos que ocorrem durante o slot de tempo especificado são encaminhados.

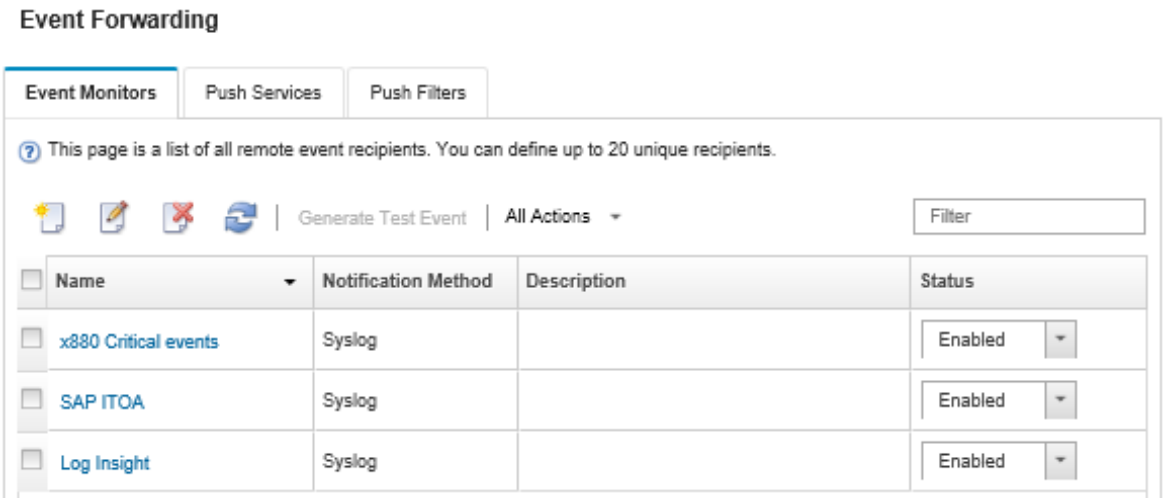
Se você não criar um planejamento para o encaminhador de evento, os eventos serão encaminhados 24h por dia/7 dias por semana.

1. Use o ícone **Rolar para a esquerda** (◀) e o ícone **Rolar para a direita** (▶), e os botões **Dia**, **Semana** e **Mês** para localizar o dia e a hora em que você deseja iniciar o planejamento.
2. Clique duas vezes no slot de tempo para abrir a caixa de diálogo Novo Período de Tempo.
3. Preencha as informações necessárias, incluindo a data e a hora de início e encerramento, e se está planejado para ocorrer novamente.
4. Clique em **Criar** para salvar o planejamento e fechar a caixa de diálogo. O novo planejamento é incluído no calendário.

Dica:
- É possível alterar o período arrastando a entrada de programação para outro período no calendário.
- É possível alterar a duração selecionando o início ou o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar o horário de encerramento selecionando o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar uma programação clicando duas vezes na entrada da programação no calendário e clicando em **Editar Entrada**.
- É possível exibir um resumo de todas as entradas da programação selecionando **Mostrar Resumo do Planejador**. O resumo inclui o período de cada entrada e quais entradas são repetíveis.
- É possível excluir uma entrada da programação do calendário ou do resumo planejador selecionando a entrada e clicando em **Excluir Entrada**.

Etapa 16. Clique em **Criar**.

O encaminhador de evento está listado na tabela Encaminhamento de Evento.



Etapa 17. Selecione o novo encaminhador de evento, clique em **Gerar Evento de Teste** e verifique se os eventos foram encaminhados corretamente para o gerenciador de SNMP remoto apropriado.

Depois de concluir

Na página Encaminhamento de Evento, é possível executar as seguintes ações em um encaminhador de evento selecionado:

- Atualizar a lista de encaminhadores de evento clicando no ícone **Atualizar** ( ).
- Exibir detalhes sobre um encaminhador de evento específico, clicando no link na coluna **Nome**.

- Alterar as propriedades do encaminhador de evento e filtrar os critérios clicando no nome do encaminhador de evento na coluna **Nome**.
- Excluir o encaminhador de evento clicando no ícone **Excluir** ( ).
- Suspender o encaminhamento de evento (consulte Suspendendo o encaminhamento de evento).
- Baixe o arquivo MIB que contém informações sobre traps SNMP clicando no ícone **Criar** ( ) e, em seguida, clique em **Baixar Arquivo MIB** na guia Geral da caixa de diálogo Novo Encaminhamento de Evento

arquivo lenovoMgrAlert.mib

Este arquivo MIB (Management Information Base) descreve os traps SNMP que o Lenovo XClarity Administrator gera, inclusive alertas que foram emitidos pelo XClarity Administrator e dispositivos gerenciados. Você pode compilar este arquivo MIB em qualquer gerenciador de trap SNMP, para que os traps SNMP enviados ao XClarity Administrator possam ser renderizados significativamente.

É possível baixar o arquivo MIB a partir da interface da Web clicando em **Monitoramento →**

Encaminhamento de Evento na barra de menus, clicando no ícone **Criar** ( ), selecionando **SNMP** para o tipo do encaminhador de evento. Em seguida, clique em **Baixar Arquivo MIB** na parte inferior da caixa de diálogo.

Os seguintes objetos são incluídos em todos os traps SNMP de saída. Objetos adicionais podem ser incluídos em alguns traps SNMP. Todos os objetos são descritos no arquivo MIB. As informações de recuperação não estão incluídas no trap.

Nota: Essa lista pode ser diferente de uma versão do XClarity Administrator para outra.
- **mgrTrapAppId**. Este é o "Lenovo Event Manager".
- **mgrTrapCommonEvtID**. ID de evento comum
- **mgrTrapDateTime**. Data e hora locais em que o evento foi gerado
- **mgrTrapEventClass**. A origem do evento. Isso pode ser Auditoria, Resfriamento, Energia, Discos, Memória, Processadores, Sistema, Teste, Adaptador, Expansão, IOModule ou Blade.
- **mgrTrapEvtID**. O identificador exclusivo do evento
- **mgrTrapFailFRUs**. Uma lista dos UUIDs de FRU com falha separados por vírgula, se aplicável
- **mgrTrapFailSNs**. Uma lista de dos números de série separados por vírgula de FRUs com falha, se aplicável.
- **mgrTrapFullyQualifiedDomainName**. O nome de domínio totalmente qualificado: o nome do host e o nome do domínio
- **mgrTrapID**. ID do trap
- **mgrTrapMsgText**. Texto de mensagem (apenas em inglês)
- **mgrTrapMsgID**. Identificador de mensagem
- **mgrTrapMtm**. Modelo e tipo do dispositivo que gerou o evento
- **mgrTrapService**. Indicador de capacidade de manutenção. Pode ser 000 (Desconhecido), 100 (Nenhum), 200 (Centro de Manutenção) ou 300 (Cliente)
- **mgrTrapSeverity**. Indicador de gravidade. Pode ser Informativo, Aviso, Menor, Grave ou Crítico
- **mgrTrapSN**. Número de série do dispositivo que gerou o evento
- **mgrTrapSrcIP**. Endereço IP do dispositivo do qual o evento gerado foi recebido
- **mgrTrapSrcLoc**. Local do dispositivo que gerou o evento, apenas em inglês (por exemplo, Slot#xx)
- **mgrTrapSrcName**. Nome do host ou nome de exibição do dispositivo que gerou o evento
- **mgrTrapSysContact**. ID de contato configurado pelo usuário
- **mgrTrapSysLocation**. Informações de local do dispositivo configurado pelo usuário
- **mgrTrapSystemName**. Nome do dispositivo, nome do componente e local do slot
- **mgrTrapTxtId**. Nome do host ou endereço IP do servidor do Lenovo Event Manager que gerou o trap
- **mgrTrapUserid**. ID do usuário associado ao evento (se o evento for interno e a classe de eventos for Auditoria)
- **mgrTrapUuid**. UUID do dispositivo que gerou o evento

Configurando o encaminhamento de evento em um syslog

É possível configurar o Lenovo XClarity Administrator para encaminhar eventos específicos a um syslog.

Sobre esta tarefa

É possível criar e habilitar até 20 encaminhadores de evento para enviar eventos a destinatários específicos.

Se o XClarity Administrator for reinicializado após os encaminhadores de evento serem configurados, você deverá aguardar o servidor de gerenciamento para gerar novamente dados internos antes que os eventos sejam encaminhados corretamente.

Nota: Para XClarity Administrator v1.2.0 e posterior, os **Comutadores** são incluído na guia **Eventos** nas caixas de diálogo Novo Encaminhador de Eventos e Alterar Encaminhador de Eventos. Se você atualizou para 1.2.0 ou posterior de uma versão anterior, lembre-se de atualizar seus encaminhadores de evento para incluir ou excluir os eventos de RackSwitch conforme apropriado. Isso será necessário mesmo se você tiver marcado a caixa de seleção **Todos os Sistemas** para selecionar todos os dispositivos.

Procedimento

Conclua as etapas a seguir para criar um encaminhador de evento para um syslog.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Encaminhamento de Evento**. A página Encaminhamento de Evento é exibida.

Etapa 2. Clique na guia **Encaminhamento de eventos**.

Etapa 3. Clique no ícone **Criar** ( ). A guia **Geral** da caixa de diálogo Novo Encaminhador de Evento é exibida.

Etapa 4. Selecione **Syslog** como o tipo de encaminhador de evento e preencha as informações específicas do protocolo:

- Digite o nome, o host de destino e a descrição opcional para o encaminhador do evento.
- Insira a porta a ser usada para o encaminhamento de eventos. O padrão é `514`.
- Selecione o protocolo a ser usado para o encaminhamento de eventos. Este pode ser um dos valores a seguir.
  - **UDP**
  - **TCP**
- Insira o período de tempo limite (em segundos) para a solicitação. O padrão é 30 segundos.
- Opcionalmente, selecione o formato do carimbo de data/hora no syslog. Este pode ser um dos valores a seguir.
  - **Hora local**. O formato padrão, por exemplo `Fri Mar 31 05:57:18 EDT 2017`.
  - **Horário GMT**. Padrão internacional (ISO8601) para data e hora, por exemplo `2017-03-31T05:58:20-04:00`.

Etapa 5. Clique em **Formato de saída** para escolher o formato de saída dos dados de evento a serem encaminhados. As informações variam para cada tipo de encaminhador de evento.

O formato de saída de exemplo a seguir é o formato padrão para destinatários do sylog. Todas as palavras entre colchetes duplos são as variáveis que são substituídas por valores reais quando um evento é encaminhado. As variáveis disponíveis para destinatários do syslog estão listadas na caixa de diálogo Formato de Saída.

```
<8[[SysLogSeverity]]> [[EventTimeStamp]] [appl=LXCA service=[[EventService]] severity=[[EventSeverity]]
class=[[EventClass]] appladdr=[[LXCA_IP]] user=[[EventUserName]] src=[[SysLogSource]] uuid=[[UUID]]
me=[[DeviceSerialNumber]] resourceIP=[[DeviceIPAddress]] systemName=[[DeviceFullPathName]]
```

```
seq=[[EventSequenceID]] EventID=[[EventID]] CommonEventID=[[CommonEventID]]
```

É possível clicar em **Redefinir para padrões** para alterar o formato de saída novamente para os campos padrão.

Etapa 6. Selecione **Permitir eventos excluídos** para evitar que eventos excluídos sejam encaminhados ou limpe **Permitir eventos excluídos** para encaminhar eventos excluídos. Para obter mais informações, consulte Excluindo eventos.

Etapa 7. Selecione **Habilitar este encaminhador** para ativar o encaminhamento de eventos para esse encaminhador.

Etapa 8. Clique em **Avançar** para exibir a guia **Dispositivos**.

Etapa 9. Selecione os dispositivos e os grupos que deseja monitorar para este encaminhador de evento.

Dica para encaminhar eventos para todos os dispositivos gerenciados (atuais e futuros), marque a caixa de seleção **Combinar todos os sistemas**.Se você não marcar a caixa de seleção **Combinar todos os sistemas**, certifique-se que os dispositivos selecionados não tenham um DUMMY-UUID na coluna UUID. Um Dummy-UUID é atribuído para dispositivos que ainda não se recuperaram após uma reinicialização ou não foram totalmente descobertos pelo servidor de gerenciamento. Se você selecionar um dispositivo com um Dummy-UUID, o encaminhamento de evento funcionará para este dispositivo até o ponto quando o dispositivo for descoberto ou recuperado, e o Dummy-UUID é alterado para o UUID real.

Etapa 10. Clique em **Avançar** para exibir a guia **Eventos**.

Etapa 11. Selecione os filtros a serem usados para este encaminhador de evento.

- **Corresponder por categoria de evento**
  1. Para encaminhar todos os eventos de auditoria independentemente do nível de status, selecione **Inclui todos os eventos de Auditoria**.
  2. Para encaminhar todos os eventos de garantia, selecione **Inclui eventos de Garantia**.
  3. Para encaminhar todos os eventos de alteração de status de funcionamento, selecione **Incluir eventos de alteração de status**.
  4. Para encaminhar todos os eventos de atualização de status de funcionamento, selecione **Incluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja encaminhar.
  6. Insira os IDs para um ou mais eventos que você deseja que o encaminhamento seja excluído. Separe os IDs usando uma vírgula (por exemplo, `FQXHMEM0214I,FQXHMEM0214I`).
- **Faça a correspondência por código de evento**. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe diversos IDs usando uma vírgula.
- **Excluir por categoria de evento**.
  1. Para excluir todos os eventos de auditoria independentemente do nível de status, selecione **Excluir todos os eventos de Auditoria**.
  2. Para excluir todos os eventos de garantia, selecione **Excluir eventos de Garantia**.
  3. Para excluir todos os eventos de alteração de status de funcionamento, selecione **Excluir eventos de alteração de status**.
  4. Para excluir todos os eventos de atualização de status de funcionamento, selecione **Excluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja excluir.
  6. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe os IDs usando uma vírgula.
- **Exclua por código de evento**. Insira os IDs de um ou mais eventos que você deseja excluir. Separe diversos IDs usando uma vírgula.

Etapa 12. Decida se deve incluir determinados tipos de eventos.

- **Incluir Todos os Eventos de Auditoria**. Envia notificações sobre eventos de auditoria, com base nas classes de eventos e gravidades selecionadas.
- **Incluir eventos de Garantia**. Envia notificações sobre garantias.
- **Incluir eventos de alteração de status**. Envia notificações sobre alterações no status.
- **Incluir eventos de atualização de status**. Enviou notificações sobre novos alertas
- **Incluir eventos do boletim**. Envia notificação sobre novos boletins.

Etapa 13. Selecione os tipos de eventos e as gravidades sobre os quais deseja ser notificado.

Etapa 14. Selecione se deve filtrar eventos por capacidade de manutenção.

Etapa 15. Clique em **Avançar** para exibir a guia **Planejador**.

Etapa 16. **Opcional:** Defina a hora e os dias em que deseja que os eventos especificados sejam encaminhados para este encaminhador de evento. Apenas eventos que ocorrem durante o slot de tempo especificado são encaminhados.

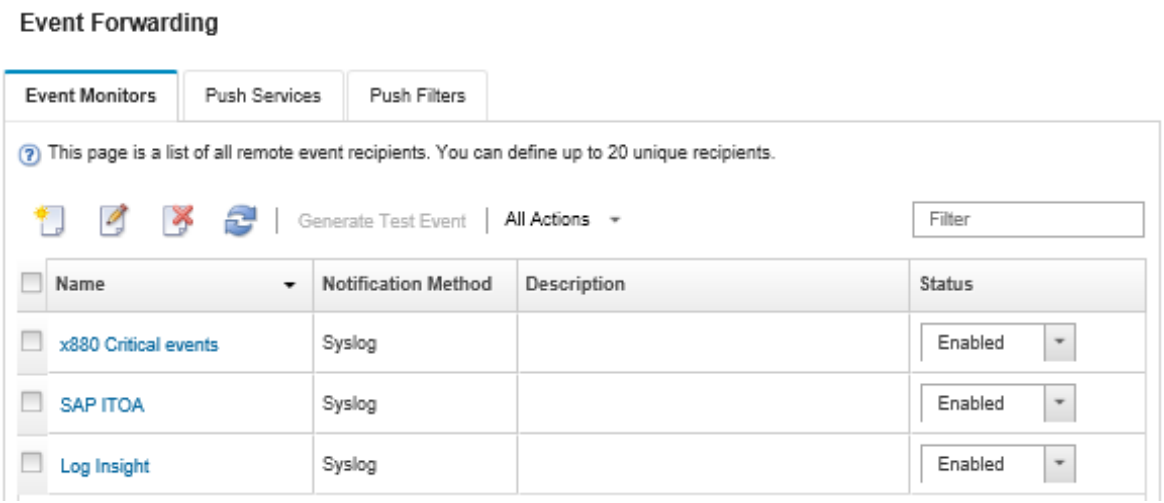
Se você não criar um planejamento para o encaminhador de evento, os eventos serão encaminhados 24h por dia/7 dias por semana.

1. Use o ícone **Rolar para a esquerda** (◀) e o ícone **Rolar para a direita** (▶), e os botões **Dia**, **Semana** e **Mês** para localizar o dia e a hora em que você deseja iniciar o planejamento.
2. Clique duas vezes no slot de tempo para abrir a caixa de diálogo Novo Período de Tempo.
3. Preencha as informações necessárias, incluindo a data e a hora de início e encerramento, e se está planejado para ocorrer novamente.
4. Clique em **Criar** para salvar o planejamento e fechar a caixa de diálogo. O novo planejamento é incluído no calendário.

Dica:
- É possível alterar o período arrastando a entrada de programação para outro período no calendário.
- É possível alterar a duração selecionando o início ou o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar o horário de encerramento selecionando o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar uma programação clicando duas vezes na entrada da programação no calendário e clicando em **Editar Entrada**.
- É possível exibir um resumo de todas as entradas da programação selecionando **Mostrar Resumo do Planejador**. O resumo inclui o período de cada entrada e quais entradas são repetíveis.
- É possível excluir uma entrada da programação do calendário ou do resumo planejador selecionando a entrada e clicando em **Excluir Entrada**.

Etapa 17. Clique em **Criar**.

O encaminhador de evento está listado na tabela Encaminhamento de Evento.



Etapa 18. Selecione o novo encaminhador de evento, clique em **Gerar Evento de Teste** e verifique se os eventos foram encaminhados corretamente para o syslog apropriado.

Depois de concluir

Na página Encaminhamento de Evento, é possível executar as seguintes ações em um encaminhador de evento selecionado:

- Atualizar a lista de encaminhadores de evento clicando no ícone **Atualizar** ( ).
- Exibir detalhes sobre um encaminhador de evento específico, clicando no link na coluna **Nome**.
- Alterar as propriedades do encaminhador de evento e filtrar os critérios clicando no nome do encaminhador de evento na coluna **Nome**.
- Excluir o encaminhador de evento clicando no ícone **Excluir** ( ).
- Suspender o encaminhamento de evento (consulte Suspendendo o encaminhamento de evento).

Suspendendo o encaminhamento de evento

É possível suspender o encaminhamento de evento, desabilitando o encaminhador de evento. Suspendendo o encaminhamento de evento, o monitoramento de eventos recebidos é interrompido. Os eventos recebidos enquanto o monitoramento está suspenso não são encaminhados.

Sobre esta tarefa

O estado desabilitado não é persistente. Se o nó de gerenciamento for reiniciado, todos os encaminhadores de evento serão habilitados.

Procedimento

Conclua as seguintes etapas para desabilitar o encaminhamento de eventos.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Monitoramento** → **Encaminhamento de Eventos**. A página Encaminhamento de Eventos é exibida.

Etapa 2. Selecione **Desabilitar** na coluna **Status** para cada encaminhador de evento que você deseja suspender.

Encaminhamento de eventos à dispositivos móveis

É possível configurar o Lenovo XClarity Administrator para enviar notificações de evento por push à dispositivos móveis

Antes de iniciar

Os requisitos a seguir devem ser atendidos para encaminhar eventos à dispositivos móveis:

- Certifique-se de que um servidor DNS válido esteja configurado para permitir que o Lenovo XClarity Administrator se conecte aos servidores push da Apple ou do Google. Isso pode ser configurado clicando em **Administração → Acesso à Internet → Editar Acesso à Rede** e, em seguida, clique na guia **Configurações de Internet** (consulte Configurando o acesso à rede na documentação online do Lenovo XClarity Administrator).
- Certifique-se de que todas as portas necessárias para o gerenciamento de evento estão abertas na rede e no firewall. Para obter informações sobre requisitos de porta, consulte Disponibilidade de porta na documentação online do Lenovo XClarity Administrator.

Sobre esta tarefa

Quando o aplicativo do Lenovo XClarity Mobile está pré-instalado em um dispositivo móvel, é possível habilitar cada instância do Lenovo XClarity Administrator conectada para enviar notificações de eventos por push para esse dispositivo móvel. Quando as notificações por push estão habilitadas para uma instância específica, é criada uma assinatura no Lenovo XClarity Administrator para esse dispositivo móvel.

É possível definir os eventos que são enviados por push para o dispositivo móvel, atribuindo filtros de evento global predefinidos ou personalizados para cada instância do Lenovo XClarity Administrator. Os filtros de evento global predefinidos são habilitados por padrão. O Lenovo XClarity Administrator inicia o monitoramento para eventos recebidos com base em critérios de filtro. Quando uma correspondência é encontrada, o evento é encaminhado ao dispositivo móvel.

Para obter mais informações sobre o Lenovo XClarity Mobile e os dispositivos móveis suportados, consulte Usando o aplicativo Lenovo XClarity Mobile na documentação online do Lenovo XClarity Administrator.

Procedimento

Para configurar as notificações por push nesse dispositivo móvel, conclua as etapas a seguir no aplicativo do Lenovo XClarity Mobile no seu dispositivo móvel.

Etapa 1. Habilite notificações por push:

- É possível habilitar notificações por push ao criar uma conexão para uma instância do Lenovo XClarity Administrator. As notificações por push são ativadas por padrão.
- É possível ativar as notificações por push em conexões existentes ativando um ou mais filtros de evento

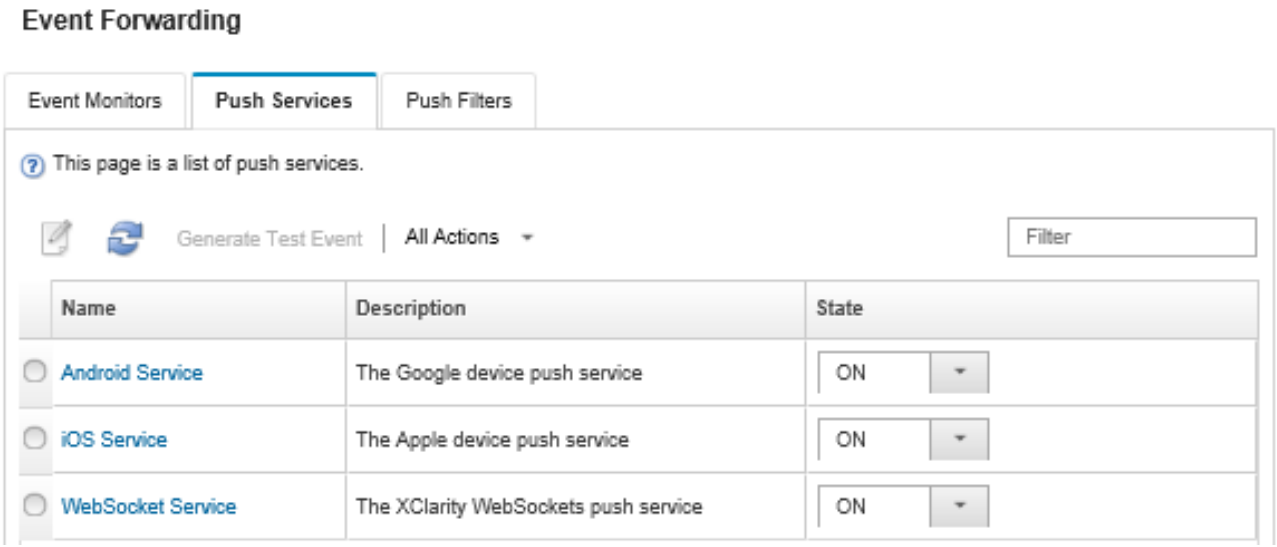
Etapa 2. Atribua filtros de evento global para especificar quais eventos devem ser encaminhados ao dispositivo móvel:

Nota: É possível incluir ou remover filtros globais de assinaturas apenas pelo aplicativo do Lenovo XClarity Mobile. É possível criar filtros globais apenas a partir da interface da Web do Lenovo XClarity Administrator. Para obter informações sobre como criar filtros de evento global personalizados, consulte Criando filtros de evento para dispositivos móveis e WebSockets.

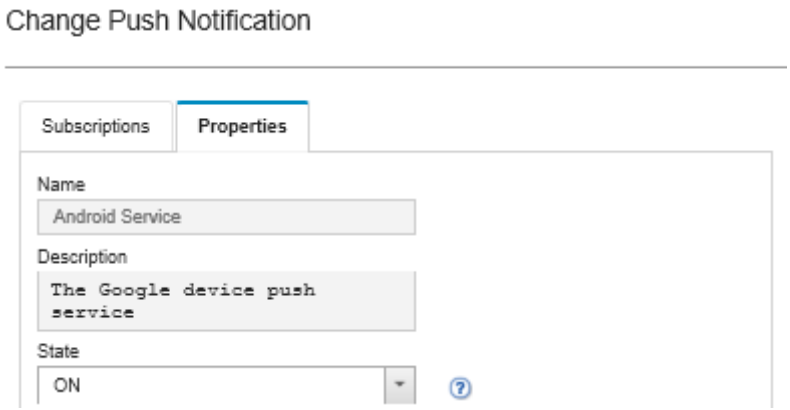
1. Toque em **Configurações → Notificações por Push**. Uma lista de conexões do Lenovo XClarity Administrator é exibida.
2. Toque na instância do Lenovo XClarity Administrator para exibir uma lista de filtros de push.
3. Habilite os filtros de evento para os eventos que você deseja que sejam enviados por push ao dispositivo móvel para a instância do Lenovo XClarity Administrator.
4. Toque em **Toque para gerar notificação por push teste** para verificar se as notificações de evento foram enviadas por push corretamente.

Resultados

É possível gerenciar assinaturas a partir da página de Encaminhamento de Evento na interface da Web do Lenovo XClarity Administrator. Clique em **Monitoramento → Encaminhamento de Eventos** para exibir a página de Encaminhamento de Eventos.



- É possível alterar propriedades do serviço de notificação do dispositivo na guia **Serviço de Push** na página de Encaminhamento de Evento. Para isso, clique no link para o serviço de notificação por push (Google ou Apple) ou na coluna **Nome** para exibir a caixa de diálogo Alterar Notificação por Push e, em seguida, clique na guia **Propriedades**.

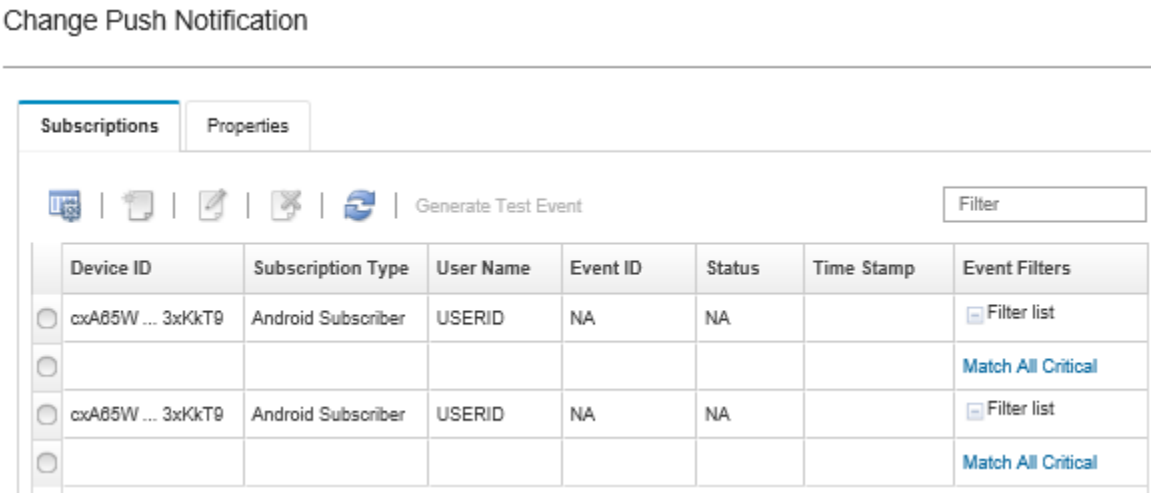


- Você pode habilitar e desabilitar as assinaturas:
  - Habilite ou desabilite todas as assinaturas para um serviço de notificação de um dispositivo específico na guia **Serviço de Push** na página de Encaminhamento de Evento selecionando o estado **ATIVADO** ou **DESATIVADO** na tabela para o serviço de notificação do dispositivo.
  - Habilite ou desabilite todas as assinaturas de um dispositivo específico a partir do aplicativo do Lenovo XClarity Mobile tocando em **Configurações → Notificação por push** e, em seguida, habilitando ou desabilitando as notificação por push.
  - Habilite ou desabilite uma assinatura específica a partir do aplicativo do Lenovo XClarity Mobile tocando em **Configurações → Notificação por push**, tocando em uma conexão de Lenovo XClarity Administrator e habilitando pelo menos um filtro de evento ou desabilitando todos os filtros de eventos.

- É possível gerar um evento de teste para todas as assinaturas para um serviço móvel específico na guia **Serviço de Push** na página Encaminhamento de Evento selecionando o serviço móvel e clicando em **Gerar Evento de Teste**.
- É possível exibir uma lista de assinaturas atuais. Na guia **Serviço de Push** na página de Encaminhamento de Evento, clique no link para o serviço de notificação do dispositivo aplicável (Android ou iOS) na coluna **Nome** para exibir a caixa de diálogo Alterar Notificação por Push e, em seguida, clique na guia **Assinaturas**. O ID do dispositivo identifica cada assinatura.

  Dicas:

  - O ID do dispositivo são os 6 primeiros e últimos dígitos do ID de registro de push. É possível localizar o ID de registro de push a partir do aplicativo Lenovo XClarity Mobile, tocando em **Configurações → Sobre → ID de registro de push**.
  - Se tiver feito login como usuário com uma das seguintes funções, todas as assinaturas serão exibidas; caso contrário, apenas as assinaturas para o usuário conectado serão exibidas.
    - **lxc-admin**
    - **lxc-supervisor**
    - **lxc-security-admin**
    - **lxc-sysmgr**
- É possível exibir a lista de filtros de evento atribuída à assinatura na guia **Assinaturas** na caixa de diálogo Alterar Notificação por Push, expandindo a **Lista de filtros** na coluna **Filtros de Evento** da assinatura.



- É possível criar filtros de evento para uma assinatura específica na guia **Assinaturas** na caixa de diálogo Alterar Notificação por Push, selecionando a assinatura e clicando no ícone **Criar** ( ).

  Nota: Esses filtros de evento se aplicam apenas a uma assinatura específica e não podem ser usados por outras assinaturas.

  Também é possível editar ou remover um filtro de evento, selecionando o filtro de evento e clicando no ícone **Editar** ( ) ou no ícone **Remover** ( ), respectivamente.
- É possível determinar o status da última tentativa por push para uma assinatura específica na guia **Assinaturas** na caixa de diálogo Alterar Notificação por Push. A coluna **Registro de data e hora** indica a data e hora do push mais recente. O **Status** indica se a notificação por push foi bem-sucedida no envio ao serviço de push. Nenhum status está disponível quanto à entrega bem-sucedida da notificação por push ao dispositivo pelo serviço. Se a entrega para o serviço de push tiver falhado, a coluna Status fornecerá informações adicionais sobre a falha.
- É possível gerar um evento de teste para uma assinatura específica na guia **Assinaturas** na caixa de diálogo Alterar Notificação por Push, selecionando a assinatura e clicando em **Gerar Evento de Teste**.

- É possível remover uma assinatura na guia **Assinaturas** na caixa de diálogo Alterar Notificação por Push, selecionando a assinatura e clicando no ícone **Remover** ( ).

Encaminhamento de eventos para serviços WebSocket

É possível configurar o Lenovo XClarity Administrator para enviar notificações de evento por push aos serviços WebSocket.

Sobre esta tarefa

As assinaturas do WebSocket não são armazenadas persistentemente em Lenovo XClarity Administrator. Quando o Lenovo XClarity Administrator é reinicializado, os assinantes do WebSocket devem assiná-lo novamente.

Procedimento

Para enviar por push a notificação de evento para um serviço WebSocket, conclua as seguintes etapas.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Monitoramento → Encaminhamento de Evento**. A página Encaminhamento de Eventos é exibida.

Etapa 2. Clique na guia **Serviços de Push**.

Etapa 3. Clique no link do **Serviço WebSocket** na coluna **Nome**. A caixa de diálogo Alterar Notificação por Push é exibida.

Etapa 4. Clique na guia **Assinaturas**.

Etapa 5. Clique no ícone **Criar** ( ).

Etapa 6. Insira o endereço IP do host de destino.

Etapa 7. Clique em **Criar**.

Etapa 8. Selecione a nova assinatura, clique em **Gerar Evento de Teste** e, em seguida, verifique se os eventos foram encaminhados corretamente ao serviço WebSocket.

Resultados

Na guia **Assinaturas**, na caixa de diálogo Alterar Notificação por Push, é possível executar as seguintes ações em uma assinatura do WebSocket selecionada:

- Atualizar a lista de serviços WebSocket clicando no ícone **Atualizar** ( ).
- Exclua as assinaturas, selecionando-as e clicando no ícone **Excluir** ( ).
- Determine o status da última tentativa de push de uma assinatura específica, visualizando o conteúdo da coluna **Status**. Se a tentativa falhar, esta coluna irá conter uma mensagem que descreverá o erro.

Na guia **Propriedades**, na caixa de diálogo Alterar Notificação por Push, é possível executar as seguintes ações:

- Altere as propriedades do serviço WebSocket, incluindo tempo de inatividade de conexão, o tamanho máximo de buffer, o número máximo de assinantes e o período limite para se registrar.
- É possível redefinir o serviço WebSocket às configurações padrão, clicando em **Restaurar Padrões**.
- Suspenda o enviar por push de notificações de evento a todas as assinaturas para o serviço WebSocket, configurando o **Estado** como Desligado.

Na guia **Serviço de Push** na página Encaminhamento de Evento, é possível gerar um evento de teste para todas as assinaturas do WebSocket, selecionando o serviço WebSocket e clicando em **Gerar Evento de Teste**.

Criando filtros de evento para dispositivos móveis e WebSockets

É possível criar filtros de eventos globais que podem ser usados em uma ou várias assinaturas para dispositivos móveis e WebSockets. Também é possível criar filtros de evento que são exclusivos a uma assinatura.

Antes de iniciar

Você deve ter autoridade de supervisor para criar filtros de evento.

É possível criar até 20 filtros de evento global.

Sobre esta tarefa

Os seguintes filtros de evento global são predefinidos:

- **Corresponda a Todos Alertas Críticos**. Este filtro corresponde a todos os eventos críticos gerados por qualquer dispositivo gerenciado ou pelo XClarity Administrator.
- **Corresponda a Todos os Avisos**. Este filtro corresponde a todos os eventos de aviso gerados por qualquer dispositivo gerenciado ou pelo XClarity Administrator.

Procedimento

Para criar um filtro de evento global, conclua as etapas a seguir.

- Crie um filtro de evento global que pode ser usado por qualquer assinatura.
  1. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Encaminhamento de Evento**. A página Encaminhamento de Eventos é exibida.
  2. Clique na guia **Filtros de Push**.
  3. Clique no ícone **Criar** ( ). A guia **Geral** da caixa de diálogo Novo Filtro de Push é exibida.
  4. Especifique a descrição de nome e a opção para este novo filtro de evento.
  5. Clique em **Avançar** para exibir a guia **Sistemas**.
  6. Selecione os dispositivos que você deseja monitorar.

     Dica para encaminhar eventos para todos os dispositivos gerenciados (atuais e futuros), marque a caixa de seleção **Combinar todos os sistemas**.Se você não marcar a caixa de seleção **Combinar todos os sistemas**, certifique-se que os dispositivos selecionados não tenham um DUMMY-UUID na coluna UUID. Um Dummy-UUID é atribuído para dispositivos que ainda não se recuperaram após uma reinicialização ou não foram totalmente descobertos pelo servidor de gerenciamento. Se você selecionar um dispositivo com um Dummy-UUID, o encaminhamento de evento funcionará para este dispositivo até o ponto quando o dispositivo for descoberto ou recuperado, e o Dummy-UUID é alterado para o UUID real.
  7. Clique em **Avançar** para exibir a guia **Eventos**.
  8. Selecione os componentes e as severidades para qual deseja que os eventos sejam encaminhados.

     Dica:
     - Para encaminhar todos os eventos de hardware, selecione **Corresponder todos os eventos**.
     - Para encaminhar eventos de auditoria, selecione **Incluir Todos os Eventos de Auditoria**.
     - Para encaminhar eventos de garantia, selecione **Inclui eventos de Garantia**.
  9. Clique em **Criar**.
- Crie um filtro de evento para uma assinatura específica:

1. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Encaminhamento de Evento**. A página Novo Encaminhamento de Eventos é exibida.
2. Clique na guia **Filtros de Push**.
3. Selecione o link para o tipo de dispositivo móvel (Android ou iOS) na coluna Nome da tabela. A caixa de diálogo Alterar Notificação por Push é exibida.
4. Clique na guia **Assinaturas** para exibir uma lista de assinaturas ativas.
5. Selecione a assinatura e clique no ícone **Criar** ( ). A guia **Geral** da caixa de diálogo Novo Filtro de Evento é exibida.
6. Especifique a descrição de nome e a opção para este novo filtro de evento.
7. Clique em **Avançar** para exibir a guia **Sistemas**.
8. Selecione os dispositivos que você deseja monitorar.

   Dica para encaminhar eventos para todos os dispositivos gerenciados (atuais e futuros), marque a caixa de seleção **Combinar todos os sistemas**.Se você não marcar a caixa de seleção **Combinar todos os sistemas**, certifique-se que os dispositivos selecionados não tenham um DUMMY-UUID na coluna UUID. Um Dummy-UUID é atribuído para dispositivos que ainda não se recuperaram após uma reinicialização ou não foram totalmente descobertos pelo servidor de gerenciamento. Se você selecionar um dispositivo com um Dummy-UUID, o encaminhamento de evento funcionará para este dispositivo até o ponto quando o dispositivo for descoberto ou recuperado, e o Dummy-UUID é alterado para o UUID real.
9. Clique em **Avançar** para exibir a guia **Eventos**.
10. Selecione os componentes e as severidades para qual deseja que os eventos sejam encaminhados.

    Dica:
    - Para encaminhar todos os eventos de hardware, selecione **Corresponder todos os eventos**.
    - Para encaminhar eventos de auditoria, selecione **Incluir Todos os Eventos de Auditoria**.
    - Para encaminhar eventos de garantia, selecione **Inclui eventos de Garantia**.
11. Clique em **Criar**.

Depois de concluir

Na guia Filtros de Push, na página de Encaminhamento de Evento, é possível executar as seguintes ações em um filtro de evento selecionado:

- Atualizar a lista de filtros de evento, clicando no ícone **Atualizar** ( ).
- Exibir detalhes sobre um filtro de evento específico, clicando no link na coluna **Nome**.
- Alterar as propriedades do filtro de evento e os critérios do filtro, clicando no ícone **Editar** ( ).

Excluir os filtros de evento, clicando no ícone **Excluir** ( ).

Trabalhando com trabalhos

Trabalhos são tarefas de execução mais longa que são executadas em um ou mais dispositivos. Você pode programar alguns trabalhos para serem executados apenas uma vez (imediatamente ou mais tarde), de maneira recorrente, ou quando ocorre um evento específico.

Trabalhos executados em segundo plano. É possível ver o status de cada tarefa no log de trabalhos.

Monitorando trabalhos

É possível exibir um log de todos os trabalhos que são iniciados pelo Lenovo XClarity Administrator. O log de trabalhos inclui os trabalhos que estão em execução, que foram concluídos ou têm erros.

Sobre esta tarefa

Trabalhos são tarefas de execução mais longa que são executadas em um ou mais dispositivos. Por exemplo, se você implantar um sistema operacional em diversos servidores, cada implantação de servidor será listada como um trabalho separado.

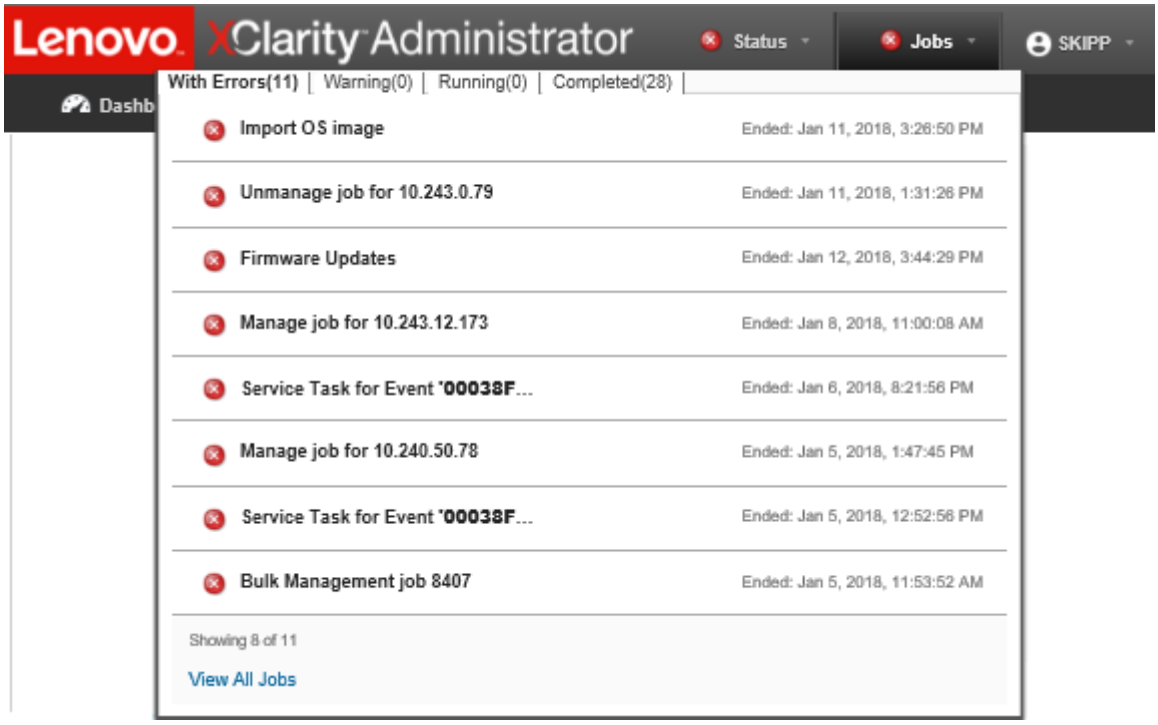
Trabalhos executados em segundo plano. É possível ver o status de cada tarefa no log de trabalhos.

O log de trabalhos contém informações sobre cada trabalho. O log pode conter no máximo 1000 trabalhos ou 1 GB. Quando o tamanho máximo for atingido, os trabalhos mais antigos concluídos com êxito serão excluídos. Se não houver nenhum trabalho concluído com êxito no log, os trabalhos mais antigos concluídos com avisos serão excluídos. Se não houver nenhum trabalho concluído com êxito nem com avisos no log, os trabalhos mais antigos concluídos com erros serão excluídos.

Procedimento

Conclua uma destas etapas para exibir o log de trabalhos.

- Na barra de título XClarity Administrator, clique em **Trabalhos** para exibir um resumo de trabalhos que estão em execução, concluídos e que têm erros.



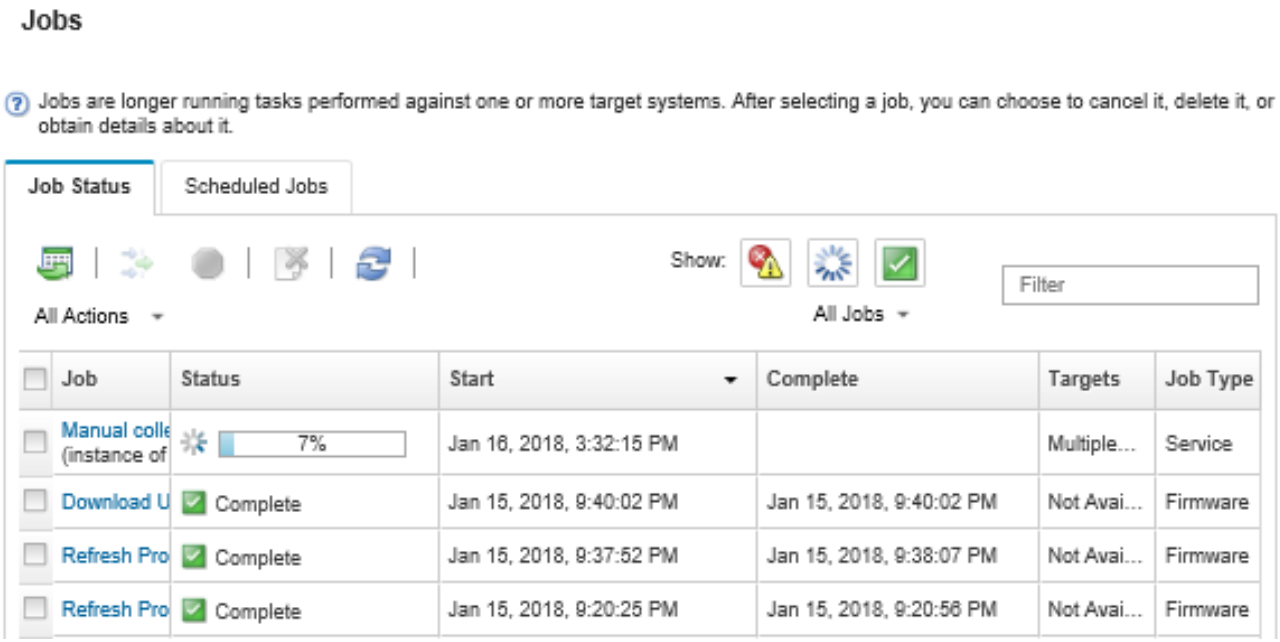
  Nesse menu, você pode clicar nas seguintes guias:
  - **Erros**. Exibe uma lista de todos os trabalhos com os erros associados.
  - **Avisos**. Exibe uma lista de todos os trabalhos com os avisos associados.
  - **Em execução**. Exibe uma lista de todos os trabalhos que estão atualmente em andamento.
  - **Concluído**. Exibe uma lista de todos os trabalhos que foram concluídos.

Passe o ponteiro do mouse sobre uma entrada de trabalho no menu para obter mais informações sobre o trabalho, incluindo o status, andamento e o usuário que criou o trabalho.

- Na barra de título do XClarity Administrator, clique em **Trabalhos** e clique no link **Exibir todos os trabalhos** para exibir a página Status dos Trabalhos.
- Na barra de menu do XClarity Administrator, clique em **Monitor → Trabalhos** e clique na guia **Status do Trabalho** para exibir a página Status dos trabalhos.

Depois de concluir

A página Trabalhos é exibida com uma lista de todos os trabalhos para o XClarity Administrator.



Nesta página, é possível executar as ações a seguir:

- Crie programações de tarefa clicando na guia **Tarefas programadas** (consulte Programando trabalhos).
- Exiba mais informações sobre um trabalho específico clicando na coluna **Trabalhos**. Uma caixa de diálogo é exibida com uma lista de subtarefas (subtrabalhos) e seus destinos, um resumo dos subtarefas incluindo quaisquer ações necessárias e detalhes do log, incluindo a severidade e o carimbo de data/hora para cada mensagem. É possível ocultar ou mostrar logs para tarefas filho.
- Para trabalhos programados, exibir informações sobre a programação do trabalho clicando "neste" link na descrição do trabalho na coluna **Trabalhos**.
- Alterar o número de trabalhos que são exibidos por página. O valor padrão é 10 trabalhos. É possível exibir 25, 50 ou todos os trabalhos.
- Limitar a lista de trabalhos que são exibidos:
  - Liste apenas os trabalhos de uma origem específica clicando em **Tipos de Trabalho** e escolhendo as opções a seguir.
    - **Todos os Tipos de Trabalho**
    - **Service**
    - **Management**
    - **Configuration**
    - **Firmware**
    - **Health**

  - **Power**
  - **Acesso remoto**
  - **ID do Sistema**
  - **Imagens do SO**
  - **Implantação do SO**
  - **Exportação de Perfil de SO**
  - **Custom**
  - **Inventory**
  - **Unknown**
- Listar apenas os trabalhos programados que estão associados a um tipo de programação específico clicando em **Tipos de Programação** e escolhendo as opções a seguir.
  - **Todos os Tipos de Programação**
  - **Única**
  - **Recorrente**
  - **Acionado**
- Ocultar ou mostrar trabalhos com erros ou avisos clicando no ícone **Ocultar trabalhos com erro/avisos** ( ).
- Ocultar ou mostrar trabalhos em execução clicando no ícone **Ocultar trabalhos em execução** ( ).
- Ocultar ou mostrar trabalhos concluídos clicando no ícone **Ocultar trabalhos concluídos** ( ).
- Listar apenas os trabalhos que contêm texto específico inserindo o texto no campo **Filtro**.
- Se a filtragem for aplicada à página, remova o filtro clicando no ícone **Mostrar Todos os Trabalhos** ( ).
- Classificar os trabalhos por coluna clicando em um título de coluna.

- Exportar a lista de trabalhos como um arquivo CSV clicando no ícone **Exportar como CSV** ( ).

  Nota: Os registros de data e hora no log exportado usam a hora local que é especificada pelo navegador da Web.
- Cancelar trabalhos em execução ou subtarefas selecionando um ou mais trabalhos ou subtarefas e clicando no ícone **Interromper** ( ).

  Nota: Cancelar o trabalho pode levar vários minutos.
- Excluir trabalhos ou subtarefas concluídos do log de trabalhos selecionando um ou mais trabalhos ou subtarefas concluídos e clicando no ícone **Excluir** ( ).
- Exporte informações sobre tarefas específicas selecionando as tarefas e clicando no ícone **Exportar como CSV** ( ).
- Atualizar o log de trabalhos clicando no ícone **Atualizar** ( ).

Programando trabalhos

É possível criar programações no Lenovo XClarity Administrator para executar determinadas tarefas em momentos específicos.

Sobre esta tarefa

É possível programar os tipos de trabalho a seguir:
- Tarefas simples, como desligar e reinicializar

- Coletando dados de serviço para dispositivos específicos
- Atualizando os catálogos de atualização de firmware e do driver de dispositivo do SO do site da Lenovo
- Atualizando o catálogo de atualizações do XClarity Administrator no site da Lenovo
- Baixando firmware no site da Lenovo
- Atualizando o firmware e drivers de dispositivo do SO em dispositivos gerenciados
- Fazendo backup de dados e configurações do XClarity Administrator
- Fazendo backup e restaurando dados de configuração do comutador

Você pode programar trabalhos para serem executados:
- Apenas uma vez (imediatamente ou posteriormente)
- De maneira recorrente
- Quando ocorre um evento específico

Procedimento

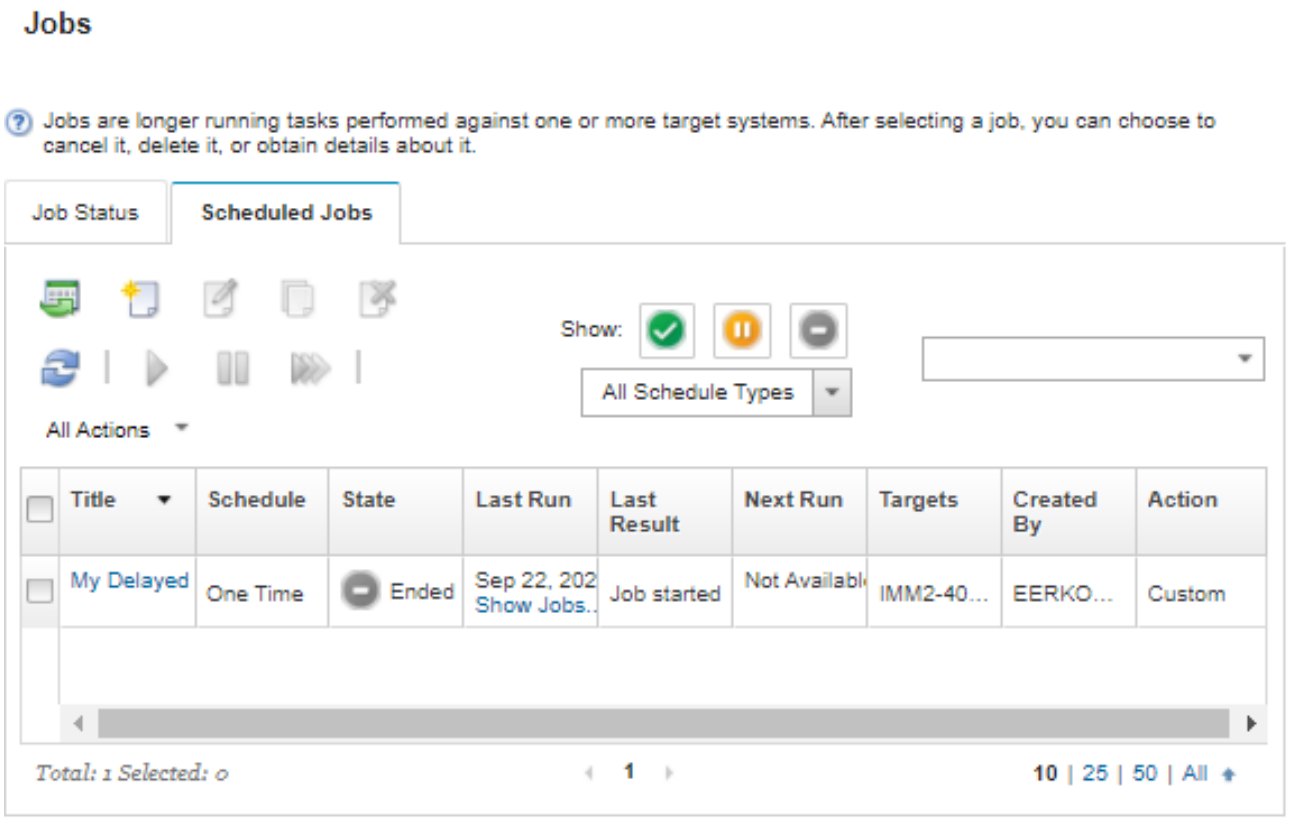
Para criar e programar um trabalho, conclua as etapas a seguir.

- Para tarefas complexas, como atualizar o firmware e coletar dados de serviço, crie o trabalho na página ou caixa de diálogo da tarefa atual.
  1. Clique em **Programação** para criar uma programação para executar essa tarefa. A caixa de diálogo Programar Novo Trabalho é exibida.
  2. Insira um nome para o trabalho.
  3. Especifique quando o trabalho deve ser executado. As opções disponíveis dependem do tipo de trabalho. Alguns trabalhos não podem ser recorrentes nem acionados por um evento
     - **Única**. Esses trabalhos são executados apenas uma vez. Especifique a data e hora em que deseja que o trabalho seja executado.
     - **Recorrente**. Esses trabalhos são executados mais de uma vez. Especifique quando e com que frequência deseja que o trabalho seja executado.
     - **Acionado pelo evento**. Esses trabalhos são executados quando ocorre um evento específico.
       a. Especifique a data e hora em que deseja que o trabalho seja executado e clique em **Avançar**.
       b. Selecione o evento para acionar o trabalho.
  4. Clique em **Criar Trabalho**.
- Para tarefas simples, como ligar e reinicializar, crie a programação do trabalho na página Trabalhos.
  1. Na barra de menu do XClarity Administrator, clique em **Monitor → Trabalhos** e clique na guia **Trabalho Programado** para exibir a página Trabalhos Programados.
  2. Clique no ícone **Criar** ( ) para exibir a caixa de diálogo Programar Novos Trabalhos.
  3. Insira um nome para o trabalho.
  4. Especifique quando o trabalho deve ser executado.
     - **Única**. Esses trabalhos são executados apenas uma vez.
       a. Especifique a data e hora em que deseja que o trabalho seja executado e clique em **Avançar**.
       b. Selecione os dispositivos gerenciados em que o trabalho deve ser executado.
     - **Recorrente**. Esses trabalhos são executados mais de uma vez.
       a. Especifique quando e com que frequência deseja que o trabalho seja executado.
       b. Selecione os dispositivos gerenciados em que o trabalho deve ser executado**.**
     - **Acionado pelo evento**. Esses trabalhos são executados quando ocorre um evento específico.
       a. Especifique a data e hora em que deseja que o trabalho seja executado e clique em **Avançar**.
       b. Selecione os dispositivos gerenciados em que o trabalho deve ser executado e clique em **Avançar**.
       c. Selecione o evento para acionar o trabalho.

5. Clique em **Criar**.

Depois de concluir

A guia Trabalhos Programados é exibida com uma lista de todas as programações de trabalho no XClarity Administrator.



Nesta página, é possível executar as ações a seguir:

- Exibir informações sobre todos os trabalhos concluídos e ativos de uma programação de trabalho específica clicando no link na coluna **Trabalho**.
  - Refinar a lista de programações de trabalho que são exibidas por um tipo de programação específico clicando em **Tipos de Programação** e escolhendo as opções a seguir:
    - **Todos os Tipos de Programação**
    - **Única**
    - **Recorrente**
    - **Acionado**
  - Ocultar ou mostrar somente programações de trabalho que estão em um estado específico clicando em um dos seguintes ícones:
    - Todos os trabalhos programados que estão ativos clicando no ícone **Ativo** ( ).
    - Todos os trabalhos programados que não estão ativos clicando no ícone **Pausado** ( ).
    - Todos os trabalhos programados que já foram executados e não estão programados para serem executados novamente clicando no ícone **Finalizado** ( ).
  - Listar apenas os trabalhos programados que contêm texto específico inserindo o texto no campo **Filtro**.

  - Classificar os trabalhos programados por coluna clicando em um título de coluna.
- Visualizar quando o trabalho foi executado pela última vez examinando a coluna **Última Execução**. Exibir o status do último trabalho executado clicando no link "Status do Trabalho" nessa coluna.
- Visualizar quando o trabalho está programado para ser executado novamente examinando a coluna **Próxima Execução**. Exibir uma lista de todas datas e horas futuras clicando no link "Mais" nessa coluna.
- Executar imediatamente o trabalho que está associado à programação clicando no ícone **Executar** ( ).
- Habilitar ou desabilitar uma programação de trabalho clicando no ícone **Pausar** ( ) ou **Ativar** ( ), respectivamente.
- Copiar e modificar uma programação de trabalho clicando no ícone **Copiar** ( ).
- Editar uma programação de trabalho clicando no ícone **Editar** ( ).
- Excluir uma ou mais programações de trabalho selecionadas clicando no ícone **Excluir** ( ).
- Exporte informações sobre programações de tarefa específicas selecionando as programações e clicando no ícone **Exportar como CSV** ( ).
- Atualizar a lista de programação do trabalho clicando em **Todas as Ações → Atualizar**.

Adicionando uma resolução e comentários a um trabalho

É possível adicionar uma resolução e comentários a um trabalho concluído, independentemente do estado de sucesso ou erro. É possível fazer isso para uma tarefa pai e para subtarefas da tarefa.

Procedimento

Conclua uma das seguintes etapas para adicionar uma resolução e comentários a um trabalho.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Monitor → Trabalhos** e clique na guia **Status do Trabalho** para exibir a página Status dos trabalhos.

Etapa 2. Clique no link para a tarefa na coluna **Tarefa** para exibir os detalhes da tarefa.

Etapa 3. Clique no ícone **Notas** ( ) para exibir a caixa de diálogo Notas.

Nessa caixa de diálogo, você pode ver um histórico de todas as notas e resoluções que foram adicionadas à tarefa. Você pode limpar o histórico clicando em **Limpar todos os registros**.

Etapa 4. Escolha uma das seguintes resoluções.
- **Sem alterações**
- **Investigação**
- **Resolvido**
- **Interrompido**

Etapa 5. Inclua um lembrete no campo **Nota**.

Etapa 6. Clique em **Aplicar**.

Na página Status da tarefa, a resolução é exibida na coluna **Status** da tarefa.

Capítulo 3. Trabalhando com serviço e suporte

A interface da Web do Lenovo XClarity Administrator fornece um conjunto de ferramentas que você pode usar para definir contatos de suporte para cada dispositivo gerenciado, coletar e enviar arquivos de serviço para Suporte da Lenovo, configurar a notificação automática para provedores de serviço quando ocorrerem certos eventos que permitem manutenção em dispositivos específicos, exibir o status do tíquete de serviço e informações de garantia. É possível entrar em contato com Suporte da Lenovo para obter ajuda e assistência técnica quando você tiver problemas.

Saiba mais: XClarity Administrator: serviço e suporte

Obtendo boletins da Lenovo

A Lenovo atualiza continuamente o site de Suporte com avisos, incluindo alertas de segurança e impacto nos serviços online. A Lenovo pode enviar esses anúncios a você como boletins na interface da Web do Lenovo XClarity Administrator.

Antes de iniciar

O XClarity Administrator deve ter acesso à Internet para receber anúncios da Lenovo.

Verifique se existe uma conexão com os endereços da Internet exigidos pelos boletins.

Sobre esta tarefa

A obtenção de boletins é habilitada por padrão.

Quando tem permissão, a Lenovo envia os seguintes tipos de boletins.
- Novas versões do XClarity Administrator ou firmware estão disponíveis
- Alertas de segurança, como vulnerabilidades, foram encontrados que afetam o firmware ou o servidor de gerenciamento
- Paralisações planejadas que afetam os serviços online do Lenovo XClarity

É possível exibir boletins de várias maneiras.

- Novos boletins são mostrados em mensagens pop-up na interface da Web do XClarity Administrator.
- Você pode visualizar uma lista de boletins dos últimos 30 dias na página Login e clicando no menu de ações do usuário (ADMIN_USER) e, em seguida, clicando em **Serviço de Boletins Lenovo**.
- É possível configurar um encaminhador de e-mail que habilite a opção **Incluir eventos do boletim** para enviar boletins por e-mail (consulte Configurando o encaminhamento de evento em um serviço de e-mail usando SMTP na documentação online do XClarity Administrator).

Procedimento

Conclua as seguintes etapas para ativar o recebimento dos boletins.

Etapa 1. Na barra de menus do Lenovo XClarity Administrator, clique em **Administração → Serviço e Suporte** e, em seguida, clique em **Serviço de Boletins Lenovo** na navegação esquerda para exibir a página Serviço de Boletim Lenovo.

Etapa 2. Selecione **Concordo em receber boletins da Lenovo**.

Etapa 3. Clique em **Aplicar**.

© Copyright Lenovo 2015, 2025

Visualizando informações sobre garantia

É possível determinar os status de garantia (inclusive garantias prolongadas) dos dispositivos gerenciados.

Antes de iniciar

O Lenovo XClarity Administrator deve ter acesso aos URLs a seguir para coletar informações sobre garantia para os dispositivos gerenciados. Verifique se não há nenhum firewall bloqueando o acesso a esses URLs. Para obter mais informações, consulte Firewalls e servidores proxy na documentação online do XClarity Administrator.

- Banco de Dados da Lenovo Warranty (internacional) – https://ibase.lenovo.com/POIRequest.aspx
- Banco de Dados da Lenovo Warranty (somente na China) – http://service.lenovo.com.cn:83/webservice/NewProductQueryService.asmx
- Serviço da Web da Lenovo Warranty – http://supportapi.lenovo.com/warranty/ ou https://supportapi.lenovo.com/warranty/

É possível ativar ou desativar essa URL de garantia em XClarity Administrator clicando em **Todas as Ações → Configurar Links de Garantia**.

Nota: Para planejamento de RackSwitch, a coluna **Número de Série** mostra o número de série qualificado.

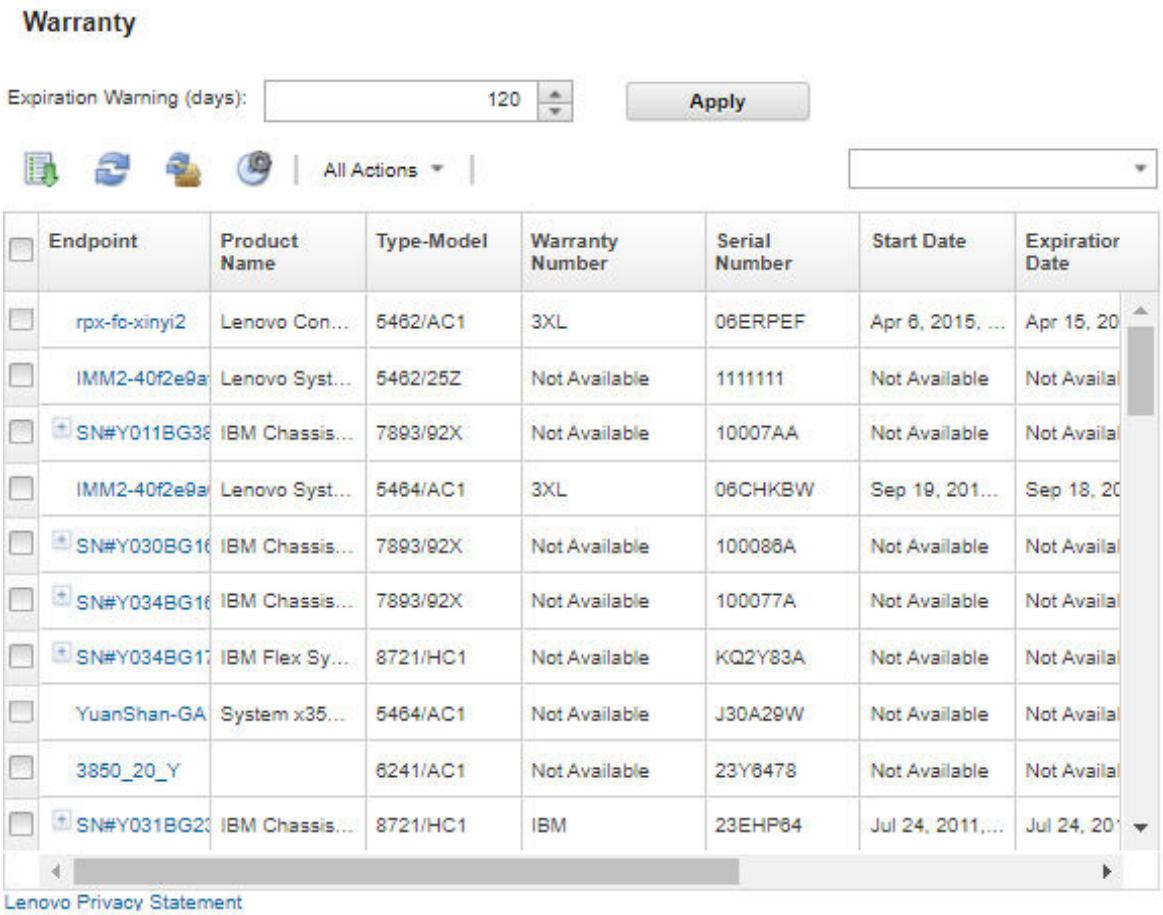
Procedimento

Para exibir o status de garantia dos dispositivos gerenciados, conclua as etapas a seguir.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Administração → Serviço e Suporte**.

Etapa 2. Clique em **Garantia** na navegação esquerda para exibir a página Garantia.

Essa página contém uma tabela que lista informações sobre garantia (como data de início, data de término e status) para cada dispositivo gerenciado.



Depois de concluir

Na página Garantia, é possível executar as ações a seguir:

- Definir quando você deseja ser avisado sobre a validade da garantia de um dispositivo gerenciado usando o campo **Aviso de expiração**. O valor padrão é 30 dias antes que a garantia expire.
- Procure as informações sobre garantia (se disponíveis) para um dispositivo específico no website de suporte da Lenovo clicando na coluna **Status**.
- Exporte o status de garantia de todos os dispositivos gerenciados para um arquivo CSV clicando no ícone **Baixar CSV** ( ).
- Atualizar as informações sobre garantia para todos os dispositivos gerenciados clicando no ícone **Atualizar Lista de Servidores** ( ).

Configurando uma notificação de problema automática

Você pode criar um encaminhador de serviços que envie dados de serviço automaticamente a seu provedor de serviço preferencial quando ocorrem determinados eventos que permitem manutenção em dispositivos gerenciados específicos. É possível enviar dados de serviço para o dispositivo ao Suporte da Lenovo (Call Home), ao técnico de serviço da Lenovo usando o Recurso de Upload da Lenovo ou a outro provedor de serviço usando o SFTP.

É possível criar e habilitar até 50 encaminhadores de serviço totais para Call Home, instalação de upload Lenovo ou SFTP.

Configurando a notificação automática do problema para o Suporte Lenovo (Call Home)

É possível criar um encaminhador de serviço que envie automaticamente dados de serviço para qualquer dispositivo gerenciado ao Suporte da Lenovo usando o Call Home quando determinados eventos que permitem manutenção são recebidos de dispositivos gerenciados específicos, como um erro de memória irrecuperável, para que o problema possa ser resolvido. Esse serviço encaminhado é chamado "Call Home Padrão."

A Lenovo está comprometida com a segurança. Quando ativado, o Call Home envia dados de serviço para o Recurso de Upload da Lenovo quando um dispositivo relata uma falha de hardware ou quando você opta por iniciar um Call Home manual. Os dados de serviço que você costuma fazer upload manualmente para o Suporte Lenovo são enviados automaticamente para o Recurso de Upload da Lenovo via HTTPS usando TLS 1.2 ou posterior; seus dados corporativos nunca são transmitidos. O acesso aos dados de serviço no Recurso de Upload da Lenovo é restrito ao pessoal de serviço autorizado.

Antes de iniciar

Atenção: Você deve aceitar a Instrução de privacidade da Lenovo para poder transferir dados para o Suporte Lenovo.

Verifique se todas as portas que são necessárias para Lenovo XClarity Administrator (incluindo as portas necessárias para Call Home) estão disponíveis antes de ativar Call Home. Para obter mais informações sobre portas, consulte Disponibilidade de porta na documentação online do XClarity Administrator.

Verifique se existe uma conexão com os endereços da Internet exigidos pelo Call Home. Para obter informações sobre firewalls, consulte Firewalls e servidores proxy na documentação online do XClarity Administrator.

Se o XClarity Administrator acessa a Internet com um proxy HTTP, verifique se o servidor proxy está configurado para usar autenticação básica e configurado como um proxy não encerrando. Para obter mais informações sobre como configurar o proxy, consulte Configurando o acesso à rede na documentação online do XClarity Administrator.

Depois de configurar Call Home, o encaminhador de serviço **Call Home da Lenovo padrão** é adicionado à página Encaminhadores de Serviço. É possível editar esse encaminhador para definir configurações adicionais, incluindo quais dispositivos estão associados a esse encaminhador. Todos os dispositivos são compatíveis com o padrão.

Atenção: Se a opção **Corresponder todos os dispositivos** estiver desabilitada, os dispositivos não selecionados de modo explícito, seja individualmente ou por meio de grupos de recursos, em nenhum encaminhador de Call Home habilitado *não* iniciarão um Call Home para o Suporte Lenovo em caso de eventos que permitam manutenção.

No momento, não há opção de Call Home de exclusão para dispositivos específicos. Na situação pouco provável de que você queira ter um subconjunto de dispositivos não Call Home para eventos que permitam manutenção, é possível criar uma mistura de grupos de recursos estáticos e dinâmicos que evitem os dispositivos pretendidos e, em seguida, adicionar esses grupos de recursos ao encaminhador de Call Home.

Atenção: Se a opção **Corresponder todos os dispositivos** não estiver habilitada para nenhum encaminhador de Call Home, o Call Home não será iniciado para nenhum dispositivo. Por essa razão, é recomendável ter pelo menos um encaminhador de Call Home com a opção **Corresponder todos os dispositivos** habilitada como um encaminhador de último recurso.

Importante:

- Quando você habilita um encaminhador de serviços Call Home no Lenovo XClarity Administrator, o Call Home é desabilitado em todos os dispositivos gerenciados para evitar a criação de registros de problema duplicados. Se você pretende deixar de usar o XClarity Administrator para gerenciar dispositivos ou se pretende desativar Call Home em XClarity Administrator, poderá reativar Call Home em todos os dispositivos gerenciados no XClarity Administrator em vez de reativar Call Home para cada dispositivo individual posteriormente. Para obter informações sobre como reabilitar o Call Home em todos os dispositivos gerenciados quando o encaminhador de serviço do Call Home estiver desativado, consulte Reativando Call Home em todos os dispositivos gerenciados
- Embora o XClarity Administrator ofereça suporte ao Call Home para dispositivos ThinkAgile e ThinkSystem, o Baseboard Management Controller para alguns dispositivos ThinkAgile e ThinkSystem não inclui suporte a Call Home. Portanto, não é possível ativar ou desativar o Call Home nesses dispositivos. O Call Home só pode ser habilitado para esses dispositivos no nível do XClarity Administrator.

Sobre esta tarefa

Um *encaminhador de serviços* define informações sobre para onde enviar os arquivos de dados de serviço quando ocorrer um evento que permite manutenção. Você pode definir até 50 encaminhadores de serviço.

- **Se um encaminhador de serviços de Call Home não estiver configurado**, você poderá abrir manualmente um tíquete de serviço e enviar os arquivos de serviço ao Centro de Suporte da Lenovo seguindo as instruções no Nova página da Web de solicitação de serviço. Para obter informações sobre como coletar e baixar arquivos de dados de serviço, consulte Coletando e baixando arquivos de serviço do Lenovo XClarity Administrator e Coletando e baixando dados de serviço de um dispositivo
- **Se um encaminhador de serviços de Call Home estiver configurado, mas não habilitado**, você poderá abrir *manualmente* um tíquete de serviço usando a função Call Home para coletar e transferir arquivos de dados de serviço ao Centro de Suporte da Lenovo a qualquer momento. Para obter mais informações, consulte Enviando uma solicitação de serviço para problemas de hardware para o Centro de Suporte da Lenovo.
- **Se um encaminhador de serviços de Call Home estiver configurado e habilitado**, o XClarity Administrator abrirá *automaticamente* um tíquete de serviço, coletará dados de serviço e os salvará como um arquivo. Depois, transferirá o arquivo de serviço para o Recurso de Upload da Lenovo quando ocorrer um evento que permite manutenção para que o problema possa ser resolvido. O arquivo de serviço do arquivo contém os dados de serviço para o dispositivo e para XClarity Administrator.

  Notas: Para Servidores ThinkSystem V3 e V4 (com XCC2 ou XCC3), o XClarity Administrator salva dados de serviço em dois arquivos no repositório.

  - **Arquivo de serviço**. (.zip) Este arquivo contém informações de serviço do dispositivo e inventário em um formato acessível com facilidade. Esse arquivo é enviado automaticamente ao Recurso de Upload da Lenovo quando ocorre um evento que permita manutenção.
  - **Arquivo de depuração**. (.tzz) O arquivo contém todas as informações de serviço do dispositivo inventário e logs de depuração para uso pelo Recurso de Upload da Lenovo. É possível enviar esse arquivo manualmente ao Suporte Lenovo se forem necessárias informações adicionais para resolver um problema.

  Para outros dispositivos, o XClarity Administrator salva dados de serviço (incluindo XClarity Administrator e informações de serviço do dispositivo, inventário e logs de depuração) em um único arquivo de serviço no repositório. Esse arquivo é enviado ao Centro de Suporte da Lenovo quando ocorre um evento que permite manutenção.

  O call home será suprimido para eventos repetidos para qualquer dispositivo se um tíquete de serviço for aberto para esse evento nesse dispositivo. O call home também será suprimido para eventos semelhantes para qualquer dispositivo ThinkAgile e ThinkSystem se um tíquete de serviço for aberto para um evento nesse dispositivo. Os eventos ThinkAgile e ThinkSystem são strings de 16 caracteres no

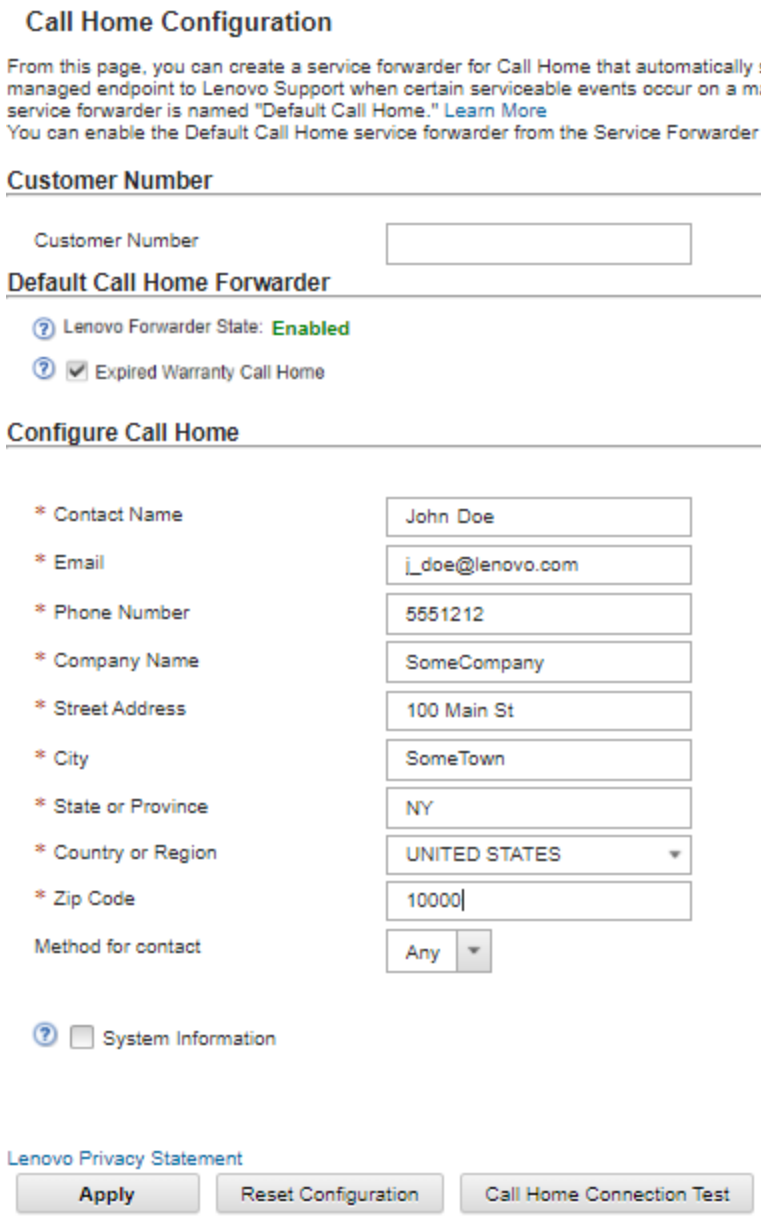
formato a seguir *xx<2_char_reading_type><2_char_sensor_type>xx<2_char_entity_ID>xxxxxx* (por exemplo, `806F010D0401FFFF`). Os eventos serão semelhantes se tiverem o mesmo tipo de leitura, tipo de sensor e ID de entidade. Por exemplo, se um tíquete de serviço for aberto para o evento 806F010D0401FFFF em um dispositivo ThinkAgile ou ThinkSystem específico, todos os eventos que ocorrerem nesse dispositivo com IDs de evento como *xx*`6F01`*xx*`04`*xxxxxx*, em que *x* é qualquer caractere alfanumérico, serão suprimidos.

Para obter informações sobre como exibir tíquetes de serviço que foram abertos automaticamente por um encaminhador de serviços de Call Home, consulte Exibindo tíquetes de serviço e o status.

Procedimento

Conclua as seguintes etapas para configurar um encaminhador de serviço para Call Home.

- Configure o Call Home para todos os dispositivos gerenciados (atuais e futuros):
  1. Na barra de menu do XClarity Administrator, clique em **Administração → Serviço e Suporte**.
  2. Clique em **Configuração de Call Home** na navegação esquerda para exibir a página Configuração de Call Home.



3. (Opcional) Especifique o número do cliente Lenovo padrão a ser usado para relatar problemas com o XClarity Administrator.

   Dica: Você pode localizar o número do seu cliente no e-mail com a prova de direito recebido ao comprar o Lenovo XClarity Pro.

4. (Opcional) Limpe **Call Home de Garantia Expirada** para impedir que os tíquetes de serviço sejam abertos automaticamente por Call Home para dispositivos com garantias expiradas.

   Nota: Essa opção não impede que você abra manualmente tíquetes de serviço para dispositivos com garantias expiradas

5. Preencha as informações de contato e local.
6. Selecione o método preferencial de contato pelo suporte da Lenovo.
7. (Opcional) Preencha as informações do sistema.
8. Clique em **Aplicar**.

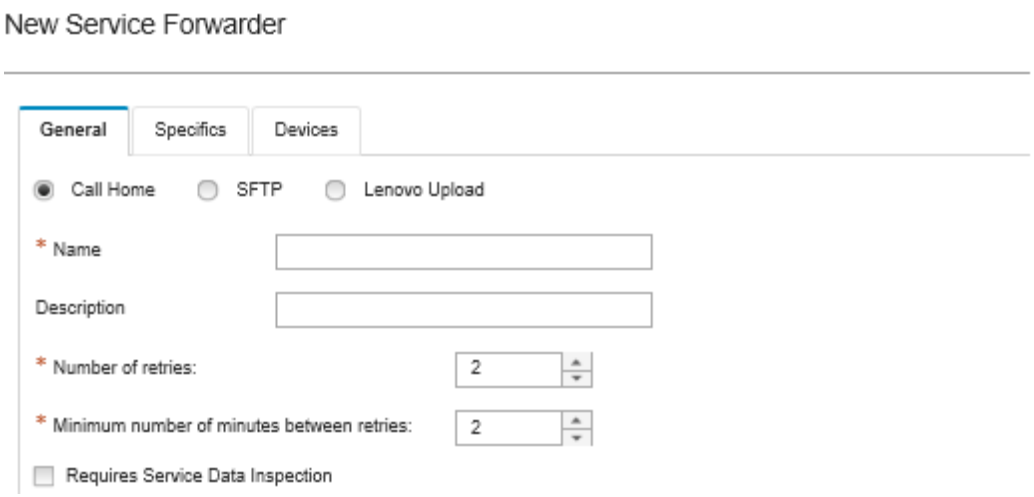
Um encaminhador de serviço do Call Home chamado "Call Home Padrão" é criado para todos os dispositivos gerenciados usando as informações de contato especificadas.

9. Ative e teste o encaminhador de serviço "Call Home Padrão".
   a. Clique em **Encaminhador de Serviços** na navegação esquerda para exibir a página Encaminhadores de Serviços.
   b. Selecione **Ativar** na coluna **Status** do encaminhador de serviço "Call Home Padrão".
   c. Selecione o encaminhador de serviço "Call Home Padrão" e clique em **Testar Encaminhadores de Serviço** para gerar um evento de teste para o encaminhador de serviço e verifique se o XClarity Administrator pode se comunicar com o Suporte Lenovo Center.

      Você pode monitorar o progresso do teste clicando em **Monitoramento → Trabalhos** na barra de menu do XClarity Administrator.

      Nota: O encaminhador de serviço deve ser habilitado antes de ser testado

- Configure o Call Home para dispositivos gerenciados específicos:
  1. Na barra de menu do XClarity Administrator, clique em **Administração → Serviço e Suporte**.
  2. Clique em **Encaminhadores de Serviços** na navegação esquerda para exibir a página Encaminhadores de Serviços.
  3. Clique no ícone **Criar Encaminhador de Serviço** ( ) para exibir a caixa de diálogo Novo Encaminhador de Serviço.
  4. Clique na guia **Geral**.

     a. Selecione **Call Home** como o encaminhador de serviço:
     b. Insira o nome de encaminhador de serviços e uma descrição.
     c. Especifique o número de novas tentativas de notificação automática. O padrão é 2.
     d. Especifique o número mínimo de minutos entre tentativas. O padrão é 2.
     e. (Opcional) Clique em **Requer Inspeção de Dados de Serviço** se desejar examinar os arquivos de dados de serviço antes que sejam transferidos e, opcionalmente, especifique o endereço de e-mail do contato que será notificado quando os arquivos de dados de serviço precisarem ser inspecionados.
  5. Clique na guia **Específico** e preencha as informações de contato e do sistema.

     Dica: Para usar as mesmas informações de contato e local configuradas na página Configuração de call home, selecione **Configuração Geral** no menu suspenso **Configuração**.

6. Clique na guia **Dispositivos** e selecione os dispositivos gerenciados e os grupos de recursos para os quais esse encaminhador de serviços deve encaminhar arquivos de serviço.

   Dica: Para encaminhar arquivos de serviço para todos os dispositivos gerenciados (atuais e futuros), marque a caixa de seleção **Corresponder todos os dispositivos**.
7. Clique em **Criar**. O encaminhador de serviço é incluído na página Serviço e Suporte.
8. Na página Encaminhadores de Serviços, selecione **Habilitar** na coluna **Status** para habilitar o encaminhador de serviços.
9. Selecione o encaminhador de serviço e clique em **Testar Encaminhadores de Serviço** para gerar um evento de teste para o encaminhador de serviço e verifique se o XClarity Administrator pode se comunicar com o Suporte Lenovo Center.

   Você pode monitorar o progresso do teste clicando em **Monitoramento → Trabalhos** na barra de menu do XClarity Administrator.

   Nota: O encaminhador de serviços deve ser ativado antes de ser testado.

Depois de concluir

Na página Serviço e Suporte, também é possível executar as ações a seguir:

- Se **Requer Inspeção de Dados de Serviço** for selecionado e um evento que permite manutenção tiver sido recebido de um dos dispositivos gerenciados associados ao encaminhador de serviço, você deverá inspecionar os arquivos de serviço antes que sejam encaminhados para o provedor de serviço. Para obter mais informações, consulte .
- Determine se o Call Home está habilitado ou desabilitado em um dispositivo gerenciado clicando em **Ações de terminal** na navegação esquerda e verificando o estado na coluna Status do **Call Home**.

  Dica: Se "Estado Desconhecido" for exibido na coluna **Call Home Status**, atualize o navegador da Web para exibir o status correto.
- Defina as informações de contato e o local do suporte para um dispositivo gerenciado específico clicando em **Ações de terminal** na navegação esquerda, selecionando o dispositivo e, em seguida, clicando no ícone **Criar perfil de contato** ( ) ou no ícone **Editar perfil de contato** ( ). As informações de contato e local para o dispositivo gerenciado estão incluídas no tíquete de serviço que o Call Home envia para o Centro de Suporte da Lenovo. Se informações exclusivas de contato e local forem especificadas para um dispositivo gerenciado, essas informações serão incluídas no tíquete de serviço. Caso contrário, as informações gerais que são especificadas para a configuração do XClarity Administrator Call Home (na página **Call Home Configuração** ou na página **Encaminhadores de Serviços**) serão usadas. Para obter mais informações, consulte Centro de Suporte da Lenovo. Para obter mais informações, consulte Definindo os contatos de suporte para dispositivos específicos.
- Exiba tíquetes de serviço que foram enviados para o Centro de Suporte da Lenovo clicando em **Status do Tíquete de Serviço** na navegação esquerda. Esta página lista os tíquetes de serviço que foram abertos automática ou manualmente por um encaminhador de serviços de Call Home, o status e os arquivos de serviço transmitidos para o Centro de Suporte da Lenovo. Para obter mais informações, consulte Exibindo tíquetes de serviço e o status.
- Colete dados de serviço para um dispositivo específico clicando em **Ações de terminal** na navegação esquerda, selecionando o dispositivo e, em seguida, clicando no ícone **Coletar Dados de Serviço** ( ). Para obter mais informações, consulte Coletando e baixando dados de serviço de um dispositivo.
- Abra manualmente um tíquete de serviço no Centro de Suporte da Lenovo, colete dados de serviço para um dispositivo específico e envie os arquivos para o Centro de Suporte da Lenovo clicando em **Ações de terminal** na navegação esquerda, selecionando o dispositivo e clicando em **Todas as Ações → Realizar**

ManualCall Home.Se o Centro de Suporte da Lenovo solicitar dados adicionais, o Suporte da Lenovo poderá instruir você a coletar novamente dados de serviço para esse ou outro dispositivo.

Para obter mais informações, consulte Enviando uma solicitação de serviço para problemas de hardware para o Centro de Suporte da Lenovo.

- Reabilite o Call Home em todos os dispositivos gerenciados clicando em **Ações de terminal** na navegação esquerda e, em seguida, clicando em **Todas as Ações → Habilitar Call Home em todos os dispositivos**.

  Quando você habilita um encaminhador de serviços Call Home no Lenovo XClarity Administrator, o Call Home é desabilitado em todos os dispositivos gerenciados para evitar a criação de registros de problema duplicados. Se você pretende deixar de usar o XClarity Administrator para gerenciar dispositivos ou se pretende desativar Call Home em XClarity Administrator, poderá reativar Call Home em todos os dispositivos gerenciados no XClarity Administrator em vez de reativar Call Home para cada dispositivo individual posteriormente.

Configurando a notificação automática de problema para o Recurso de Upload da Lenovo

É possível criar um encaminhador de serviço que envie automaticamente dados de serviço para qualquer dispositivo gerenciado ao técnico de serviços da Lenovo usando o Recurso de Upload da Lenovo quando certos eventos que permitem manutenção são recebidos de dispositivos gerenciados específicos, como um erro de memória irrecuperável, para que o problema possa ser resolvido. O encaminhador de serviço é denominado "Recurso de Upload da Lenovo Padrão."

A Lenovo está comprometida com a segurança. Seus dados corporativos nunca são transmitidos. O acesso aos dados de serviço no Recurso de Upload da Lenovo é restrito ao pessoal de serviço autorizado.

Antes de iniciar

Atenção: Você deve aceitar a Instrução de privacidade da Lenovo para poder transferir dados para o Suporte Lenovo.

Garanta que as portas que são necessárias ao Lenovo XClarity Administrator estejam disponíveis antes de configurar um encaminhador de serviço. Para obter mais informações sobre portas, consulte Disponibilidade de porta na documentação online do XClarity Administrator.

Verifique se existe uma conexão com os endereços da Internet exigidos pelo Recurso de Upload da Lenovo. Para obter informações sobre firewalls, consulte Firewalls e servidores proxy na documentação online do XClarity Administrator.

Se o XClarity Administrator acessa a Internet com um proxy HTTP, verifique se o servidor proxy está configurado para usar autenticação básica e configurado como um proxy não encerrando. Para obter mais informações sobre como configurar o proxy, consulte Configurando o acesso à rede na documentação online do XClarity Administrator.

Nota: Se vários encaminhadores de serviço forem configurados para o mesmo dispositivo, somente um deles transferirá dados de serviço. A URL de email e upload usada depende do encaminhador de serviço que é acionado primeiro.

Sobre esta tarefa

Um *encaminhador de serviços* define informações sobre para onde enviar os arquivos de dados de serviço quando ocorrer um evento que permite manutenção. Você pode definir até 50 encaminhadores de serviço.

- **Se um encaminhador de serviço do Recurso de Upload da Lenovo estiver configurado, mas não habilitado**, você poderá transferir *manualmente* os arquivos de dados de serviço coletados para o Recurso de Upload da Lenovo a qualquer momento. Para obter mais informações, consulte Enviando uma solicitação de serviço para problemas de hardware para o Centro de Suporte da Lenovo.
- **Se um encaminhador de serviços do Recurso de Upload da Lenovo estiver configurado e habilitado**, o XClarity Administrator coletará dados de serviço *automaticamente* e transferirá o arquivo de serviço ao Recurso de Upload da Lenovo quando ocorrer um evento que permite manutenção para que o problema possa ser resolvido.

  Para Servidores ThinkSystem V3 e V4 (com XCC2 ou XCC3), o XClarity Administrator salva dados de serviço em dois arquivos no repositório.

  – **Arquivo de serviço**. (.zip) Este arquivo contém informações de serviço e inventário em um formato acessível com facilidade. Esse arquivo é enviado automaticamente ao Recurso de Upload da Lenovo quando ocorre um evento que permita manutenção.

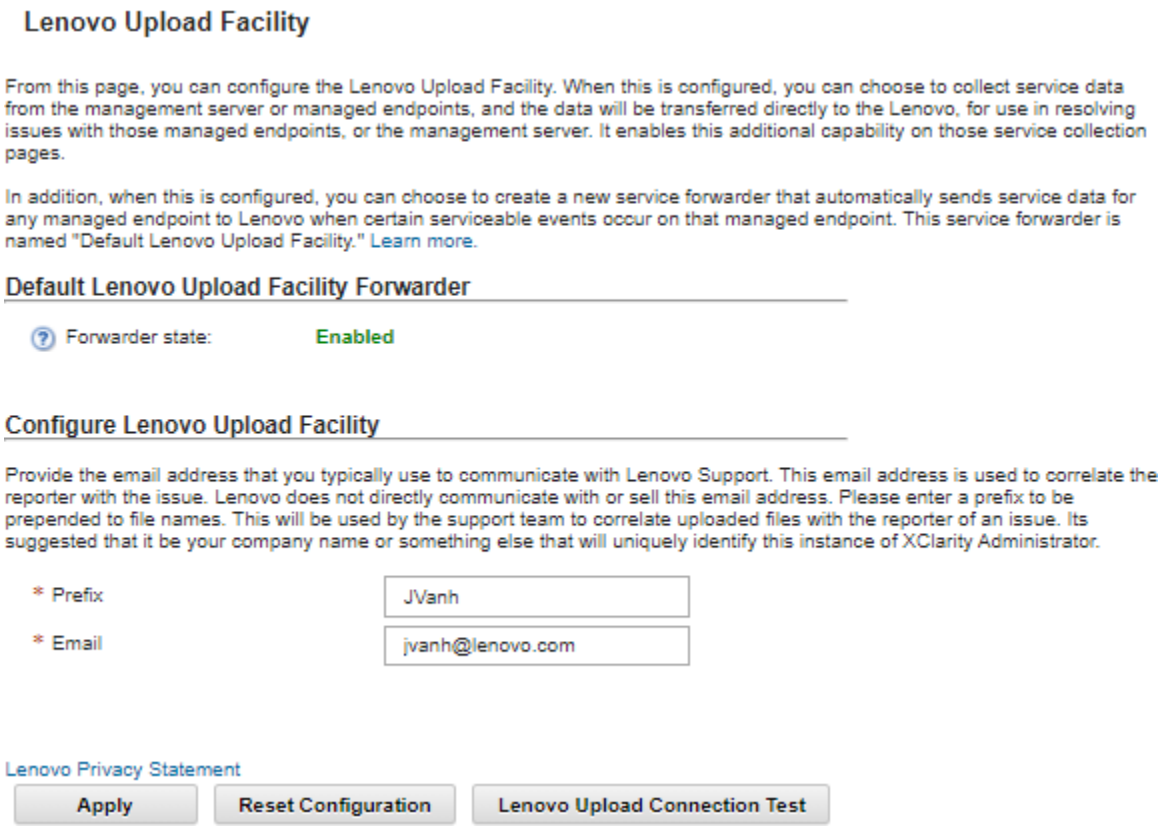
  – **Arquivo de depuração**. (.tzz) O arquivo contém todas as informações de serviço, inventário e logs de depuração para uso pelo Suporte Lenovo. É possível enviar esse arquivo manualmente ao Suporte Lenovo se forem necessárias informações adicionais para resolver um problema.

  Para outros dispositivos, o XClarity Administrator salva dados de serviço (por exemplo, informações de serviço, inventário e logs de depuração) em um único arquivo de serviço no repositório. Esse arquivo é enviado ao Recurso de Upload da Lenovo quando ocorre um evento que permita manutenção.

Procedimento

Conclua as seguintes etapas para configurar um encaminhador de serviço para o Recurso de Upload da Lenovo.

- Configure um encaminhador de serviço para o Recurso de Upload da Lenovo para todos os dispositivos gerenciados:
  1. Na barra de menu do XClarity Administrator, clique em **Administração → Serviço e Suporte**.
  2. Clique em **Recurso de Upload da Lenovo** na navegação esquerda para exibir a página Recurso de Upload da Lenovo.



3. Insira o endereço de e-mail e o URL que foram fornecidos pelo Suporte Lenovo.
4. Dê um clique em **Aplicar**.

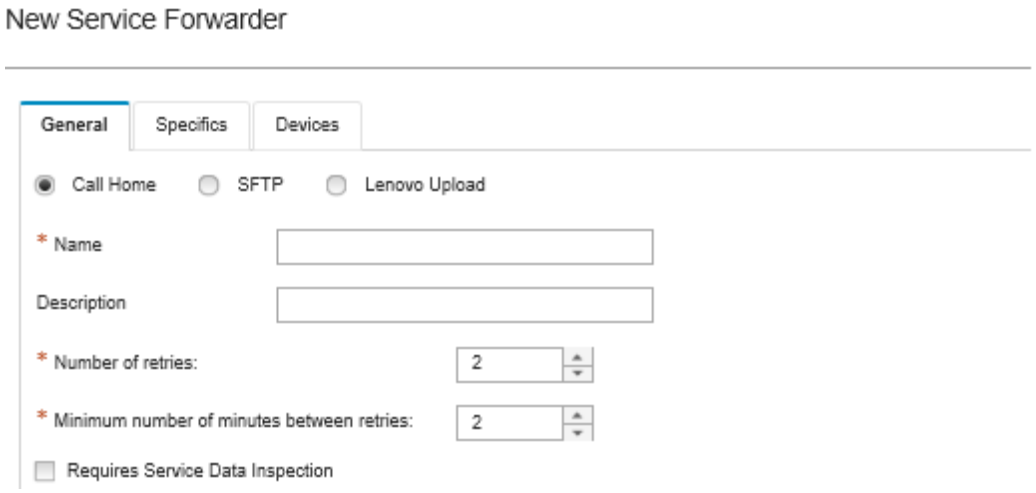
   Um encaminhador de serviço do chamado "Recurso de Upload Padrão da Lenovo" é criado para todos os dispositivos gerenciados usando as informações de contato especificadas.
5. Ative e teste o encaminhador de serviço "Recurso de Upload Padrão da Lenovo".
   a. Clique em **Encaminhadores de Serviços** na navegação esquerda para exibir a página Encaminhadores de Serviços.
   b. Selecione **Ativar** na coluna **Status** do encaminhador de serviço "Recurso de Upload Padrão da Lenovo".
   c. Selecione o encaminhador de serviço "Recurso de Upload Padrão da Lenovo" e clique em **Testar Encaminhadores de Serviço** para gerar um evento de teste para o encaminhador de serviço e verifique se o XClarity Administrator pode se comunicar com o Recurso de Upload Padrão da Lenovo.

      Você pode monitorar o progresso do teste clicando em **Monitoramento → Trabalhos** na barra de menu do XClarity Administrator.

      Nota: O encaminhador de serviços deve ser ativado antes de ser testado.

- Configure um encaminhador de serviço para o Recurso de Upload da Lenovo para dispositivos gerenciados específicos:
  1. Na barra de menu do XClarity Administrator, clique em **Administração → Serviço e Suporte**. A página Serviço e Suporte é exibida.
  2. Clique em **Encaminhadores de Serviços** na navegação esquerda para exibir a página Encaminhadores de Serviços.

3. Clique no ícone **Criar Encaminhador de Serviço** ( ) para exibir a caixa de diálogo Novo Encaminhador de Serviço.
4. Clique na guia **Geral**.



   a. Selecione **Upload da Lenovo** para o encaminhador de serviço.
   b. Insira o nome de encaminhador de serviços e uma descrição.
   c. Especifique o número de novas tentativas de notificação automática. O padrão é 2.
   d. Especifique o número mínimo de minutos entre tentativas. O padrão é 2.
   e. (Opcional) Clique em **Requer Inspeção de Dados de Serviço** se desejar examinar os arquivos de serviço antes que eles sejam transferidos e, opcionalmente, especifique o endereço de e-mail do contato que será notificado quando os arquivos de serviço precisarem ser inspecionados.
5. Clique na guia **Específico**, preencha o endereço de e-mail e a URL para upload que foi fornecida pelo Suporte Lenovo.
6. Clique na guia **Dispositivos** e selecione os dispositivos gerenciados e os grupos de recursos para os quais esse encaminhador de serviços deve encaminhar dados de serviço.

   Dica: Para encaminhar dados de serviço para todos os dispositivos gerenciados (atuais e futuros), marque a caixa de seleção **Corresponder todos os dispositivos**.
7. Clique em **Criar**. O encaminhador de serviço é incluído na página Serviço e Suporte.
8. Na página Serviço e Suporte, selecione **Ativar** na coluna **Status** para ativar o encaminhador de serviço.
9. Selecione o encaminhador de serviço e clique em **Testar Encaminhadores de Serviço** para gerar um evento de teste para cada encaminhador de serviço e verifique se o XClarity Administrator pode fazer transferências para o Recurso de Upload da Lenovo.

   Nota: O encaminhador de serviços deve ser ativado antes de ser testado.

Depois de concluir

Na página Serviço e Suporte, também é possível executar as ações a seguir:

- Se **Requer Inspeção de Dados de Serviço** for selecionado e um evento que permite manutenção tiver sido recebido de um dos dispositivos gerenciados associados ao encaminhador de serviço, você deverá inspecionar os arquivos de serviço antes que sejam encaminhados para o provedor de serviço. Para obter mais informações, consulte Inspecionando arquivos de serviço.

- Modifique as informações do encaminhador de serviços clicando em **Encaminhadores de Serviço** na navegação esquerda e clicando no ícone **Editar Encaminhador de Serviço** ( ).
- Habilite ou desabilite um provedor de serviço, clicando em **Encaminhadores de Serviços** e selecionando **Habilitar** ou **Desabilitar** na coluna **Status**.
- Exclua o provedor de serviço clicando em **Encaminhadores de Serviços** e clicando no ícone **Excluir Encaminhadores de Serviços** ( ).
- Colete dados de serviço para um dispositivo específico clicando em **Ações de terminal** na navegação esquerda, selecionando o dispositivo e, em seguida, clicando no ícone **Coletar Dados de Serviço** ( ). Para obter mais informações, consulte Coletando e baixando dados de serviço de um dispositivo.

Configurando a notificação de problema automática em um provedor de serviços preferencial

É possível criar um encaminhador de serviços que envie automaticamente dados de serviço para seu provedor de serviço preferencial usando SFTP quando determinados eventos que permitem manutenção são recebidos de dispositivos gerenciados específicos, como um erro de memória irrecuperável, para que o problema possa ser resolvido.

Antes de iniciar

Atenção: Você deve aceitar a Instrução de privacidade da Lenovo para poder transferir dados para o Suporte Lenovo.

Verifique se todas as portas que são necessárias para XClarity Administrator (incluindo as portas necessárias para call home) estão disponíveis antes de configurar um encaminhador de serviços. Para obter mais informações sobre portas, consulte Disponibilidade de porta na documentação online do XClarity Administrator.

Verifique se existe uma conexão com os endereços da Internet exigidos pelo provedor de serviço.

Se você optar por usar o Suporte da Lenovo, verifique se existe uma conexão com os endereços da Internet exigidos pelo Call Home. Para obter informações sobre firewalls, consulte Firewalls e servidores proxy na documentação online do XClarity Administrator.

Se o XClarity Administrator acessa a Internet com um proxy HTTP, verifique se o servidor proxy está configurado como um proxy não encerrando. Para obter mais informações sobre como configurar o proxy, consulte Configurando o acesso à rede na documentação online do XClarity Administrator.

Sobre esta tarefa

Um *encaminhador de serviços* define informações sobre para onde enviar os arquivos de dados de serviço quando ocorrer um evento que permite manutenção. Você pode definir até 50 encaminhadores de serviço.

Para cada encaminhador de serviço, é possível transferir automaticamente dados de serviço ao Suporte Lenovo (denominado *Call Home*), ao Recurso de Upload da Lenovo ou a outro provedor de serviço usando o SFTP. Para obter informações sobre a configuração de um encaminhador de serviço para o Call Home, consulte Configurando uma notificação de problema automática. Para obter informações sobre a configuração de um encaminhador de serviço para o Recurso de Upload da Lenovo, consulte Configurando a notificação automática de problema para o Recurso de Upload da Lenovo.

Se um encaminhador de serviço estiver configurado e ativado para SFTP, o XClarity Administrator coletará *automaticamente* os dados de serviço e transferirá os arquivos de serviço ao site de SFTP especificado do provedor de serviço preferencial.

Para Servidores ThinkSystem V3 e V4 (com XCC2 ou XCC3), o XClarity Administrator salva dados de serviço em dois arquivos no repositório.

- **Arquivo de serviço**. (.zip) Este arquivo contém informações de serviço e inventário em um formato acessível com facilidade. Esse arquivo é enviado automaticamente ao provedor de serviço preferencial quando ocorre um evento que permita manutenção.
- **Arquivo de depuração**. (.tzz) O arquivo contém todas as informações de serviço, inventário e logs de depuração para uso pelo Suporte Lenovo. É possível enviar esse arquivo manualmente ao Suporte Lenovo se forem necessárias informações adicionais para resolver um problema.

Para outros dispositivos, o XClarity Administrator salva dados de serviço (por exemplo, informações de serviço, inventário e logs de depuração) em um único arquivo de serviço no repositório. Esse arquivo é enviado ao provedor de serviço preferencial quando ocorre um evento que permita manutenção.

Nota: Se vários encaminhadores de serviço SFTP forem configurados para o mesmo dispositivo, somente um deles transferirá dados de serviço. O endereço e a porta usados dependem do encaminhador de serviço que é acionado primeiro.

Procedimento

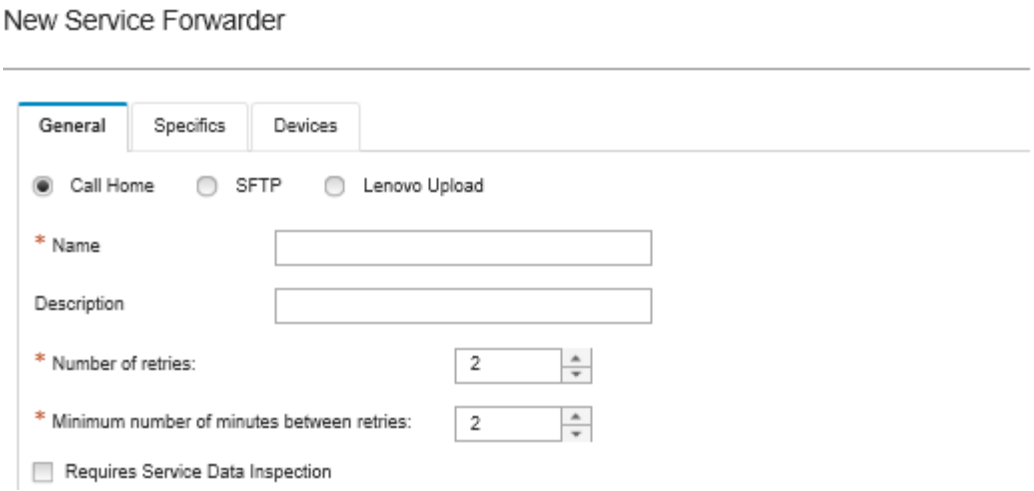
Conclua as seguintes etapas para configurar e ativar um encaminhador de serviços.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Administração → Serviço e Suporte**. A página Serviço e Suporte é exibida.

Etapa 2. Clique em **Encaminhadores de Serviços** na navegação esquerda para exibir a página Encaminhadores de Serviços.

Etapa 3. Clique no ícone **Criar Encaminhador de Serviço** ( ) para exibir a caixa de diálogo Novo Encaminhador de Serviço.

Etapa 4. Clique na guia **Geral**.



1. Selecione **SFTP** para o encaminhador de serviço:
2. Insira o nome de encaminhador de serviços e uma descrição.
3. Especifique o número de novas tentativas de notificação automática. O padrão é `2`.
4. Especifique o número mínimo de minutos entre tentativas. O padrão é `2`.

5. (Opcional) Clique em **Requer Inspeção de Dados de Serviço** se desejar examinar os arquivos de serviço antes que eles sejam transferidos e, opcionalmente, especifique o endereço de e-mail do contato que será notificado quando os arquivos de serviço precisarem ser inspecionados.

Etapa 5. Clique na guia **Específico** e preencha as seguintes informações:
- Endereço IP e número da porta do servidor SFTP
- ID do usuário e senha para autenticação no servidor SFTP

Etapa 6. Clique na guia **Dispositivo** e selecione os dispositivos gerenciados e os grupos de recursos para os quais esse encaminhador de serviços deve encaminhar dados de serviço.

Dica: Para encaminhar dados de serviço para todos os dispositivos gerenciados (atuais e futuros), marque a caixa de seleção **Corresponder todos os dispositivos**.

Etapa 7. Clique em **Criar**. O encaminhador de serviço é incluído na página Serviço e Suporte

Etapa 8. Na página Serviço e Suporte, selecione **Ativar** na coluna **Status** para ativar o encaminhador de serviços.

Etapa 9. Para evitar que os eventos que permitem manutenção que estão na lista de eventos excluídos abram relatórios de problemas automaticamente, selecione **Não** ao lado da pergunta **Deseja que os eventos excluídos abram relatórios de problemas?**.

Etapa 10. Selecione o encaminhador de serviço e clique em **Testar Encaminhadores de Serviço** para gerar um evento de teste para o encaminhador de serviço e verifique se XClarity Administrator pode se comunicar com cada provedor de serviço.

Nota: O encaminhador de serviços deve ser ativado antes de ser testado.

Depois de concluir

Na página Serviço e Suporte, também é possível executar as ações a seguir:

- Se **Requer Inspeção de Dados de Serviço** for selecionado e um evento que permite manutenção tiver sido recebido de um dos dispositivos gerenciados associados ao encaminhador de serviço, você deverá inspecionar os arquivos de serviço antes que sejam encaminhados para o provedor de serviço. Para obter mais informações, consulte Inspecionando arquivos de serviço.
- Modifique as informações do encaminhador de serviços clicando em **Encaminhadores de Serviço** na navegação esquerda e clicando no ícone **Editar Encaminhador de Serviço** ( ).
- Habilite ou desabilite um provedor de serviço, clicando em **Encaminhadores de Serviços** e selecionando **Habilitar** ou **Desabilitar** na coluna **Status**.
- Exclua o provedor de serviço clicando em **Encaminhadores de Serviços** e clicando no ícone **Excluir Encaminhador de Serviço** ( ).
- Defina as informações de contato e o local do suporte para um dispositivo gerenciado específico clicando em **Ações de terminal** na navegação esquerda, selecionando o dispositivo e, em seguida, clicando no ícone **Criar perfil de contato** ( ) ou no ícone **Editar perfil de contato** ( ). As informações de contato e local para o dispositivo gerenciado estão incluídas no registro de problemas criado por call home no Centro de Suporte da Lenovo. Se informações exclusivas de contato e local forem especificadas para um dispositivo gerenciado, essas informações serão incluídas no registro de problemas. Caso contrário, as informações gerais especificadas para a configuração de call home do XClarity Administrator (na página **Configuração de Call Home** ou na página **Encaminhadores de Serviço**) serão usadas. Para obter mais informações, consulte Definindo os contatos de suporte para dispositivos específicos.
- Colete dados de serviço para um dispositivo específico clicando em **Ações de terminal**, selecionando o dispositivo e, em seguida, clicando no ícone **Coletar Dados de Serviço** ( ). Para obter mais informações, consulte Coletando e baixando dados de serviço de um dispositivo.

Para obter mais informações sobre essas tarefas de serviço e suporte, consulte Trabalhando com serviço e suporte.

Alterando a senha de recuperação de serviço

Se o Lenovo XClarity Administrator não responder e não for possível recuperá-lo, será possível coletar e baixar dados de serviço e logs para essa instância do XClarity Administrator. A senha de recuperação de serviço é necessária para acessar o serviço para coletar e baixar dados.

Antes de iniciar

Você deve ter autoridade **lxc-service-admin** ou **lxc-supervisor** para alterar a senha.

Nota: Certifique-se de gravar a senha para uso posterior. Não é possível recuperar um hub de gerenciamento não responsivo sem usar essa senha.

Para obter mais informações sobre como usar a senha de recuperação de serviço, consulte Coletando e baixando arquivos de serviço para um Lenovo XClarity Administrator que não responde.

Procedimento

Para alterar a senha de recuperação de serviço, conclua as seguintes etapas.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Administração → Serviço e Suporte**. A página Serviço e Suporte é exibida.

Etapa 2. Clique em **Senha de recuperação de serviço** na navegação esquerda para exibir a página Senha de recuperação de serviço.

Etapa 3. Digite a nova senha

As senhas devem ter de **16** a **256** caracteres, incluindo um ou mais caracteres alfabéticos maiúsculas e inferiores, números e caracteres especiais.

Etapa 4. Clique em **Aplicar**.

Inspecionando arquivos de serviço

É possível configurar um encaminhador de serviço para que os arquivos de serviço sejam inspecionados e aceitos antes de serem enviados.

Sobre esta tarefa

A coluna **Requer Atenção** na tabela do encaminhador de serviços identifica se os arquivos de serviço requerem inspeção antes de serem encaminhados para o provedor de serviço. Se um ou mais arquivos de serviço estiverem disponíveis para inspeção, **Sim** será exibido na coluna. Caso contrário, **Não** será exibido.

Procedimento

Conclua as etapas a seguir para encaminhar arquivos de serviço específicos para o provedor de serviço.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Administração → Serviço e Suporte**. A página Serviço e Suporte é exibida.

Etapa 2. Clique em **Encaminhadores de Serviços** na navegação esquerda para exibir uma tabela de encaminhadores de serviços.

Etapa 3. Clique no link **Sim** na coluna **Requer Atenção** para exibir a caixa de diálogo Atenção Necessária com uma lista de arquivos de serviço que requerem inspeção.

Etapa 4. Selecione um ou mais arquivos de serviço e clique em **Baixar** para baixar e inspecionar o arquivo.

Etapa 5. Selecione um ou mais arquivos de serviço novamente e clique em Aceitar para iniciar a transferência do arquivo para o provedor de serviço configurado.

Nota: Se você escolher **Recusar**, os arquivos de serviço serão removidos da caixa de diálogo Requer Atenção , mas permanecerão no repositório até serem excluídos.

Definindo os contatos de suporte para dispositivos específicos

Especificar informações de contato de suporte que sejam exclusivas de um ou mais dispositivos específicos é importante quando os dispositivos são administrados por vários usuários.

Sobre esta tarefa

Se informações de contato de suporte forem definidas para um dispositivo, as informações específicas do dispositivo serão incluídas nos registros de problemas que são abertos automaticamente pelo Call Home para esse dispositivo. Se as informações específicas do dispositivo não forem definidas, as informações de contato gerais para o Lenovo XClarity Administrator que são definidas na página **Encaminhadores de Serviço** ou na página **Call Home Configuração** serão incluídas.

Procedimento

Conclua as seguintes etapas para definir as informações de contato de suporte e local de um dispositivo específico.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Administração → Serviço e Suporte**. A página Serviço e Suporte é exibida.

Etapa 2. Clique em **Ações de terminal** na navegação esquerda para exibir a página Ações de terminal

Etapa 3. Selecione um ou mais dispositivos e clique no ícone **Criar Perfil de Contato** ( ) para exibir a caixa de diálogo Criar Perfil de Contato.

Etapa 4. Preencha os campos obrigatórios e clique em **Salvar**.

Depois de concluir

Após definir informações de contato para um dispositivo, você poderá alterar ou excluir as informações de contato selecionando o dispositivo e clicando no ícone **Editar perfil de contato** ( ) ou no ícone **Excluir Perfil de Contato** ( ).

Nota: Se não existe um perfil de contato para o dispositivo selecionado, a caixa de diálogo Criar Perfil de Contato é exibida quando você tenta editar o perfil.

Coletando e baixando dados de serviço de um dispositivo

Quando há um problema em um dispositivo gerenciado que requeira a assistência de um provedor de serviço para ser resolvido, é possível usar a interface da Web do Lenovo XClarity Administrator para coletar manualmente dados de serviço (incluindo logs de depuração, informações de serviço e inventário) para esse dispositivo para ajudar a identificar a causa do problema. Os dados de serviço são salvos como um arquivo de serviço em formato tar.gz. É possível baixar ou enviar os arquivos de serviço para o provedor de serviços preferencial.

Sobre esta tarefa

Você pode executar até 20 processos de coleta de dados de serviço por vez.

Para Servidores ThinkSystem V3 e V4 (com XCC2 ou XCC3), o XClarity Administrator salva dados de serviço em dois arquivos no repositório.

- **Arquivo de serviço**. (.zip) Este arquivo contém informações de serviço e inventário em um formato acessível com facilidade.
- **Arquivo de depuração**. (.tzz) O arquivo contém todas as informações de serviço, inventário e logs de depuração para uso pelo Suporte Lenovo.

Para outros dispositivos, o XClarity Administrator salva dados de serviço (por exemplo, informações de serviço, inventário e logs de depuração) em um único arquivo de serviço no repositório.

Quando um dispositivo gerenciado gera um evento que permite manutenção que aciona o Call Home (consulte Eventos de hardware que notificam automaticamente o Suporte na documentação online do XClarity Administrator), XClarity Administrator coleta automaticamente os dados de serviço para esse dispositivo. Se um encaminhador de serviço estiver configurado e habilitado, o XClarity Administrator também enviará o arquivo de serviço ao provedor de serviço especificado (por exemplo, o Centro de Suporte da Lenovo usando o Call Home ou um site de SFTP). Se o provedor de serviço precisar de dados adicionais, você poderá ser instruído a coletar novamente dados de serviço desse ou de outro dispositivo usando o procedimento descrito abaixo.

Quando o repositório de dados de serviço atinge sua capacidade máxima, o conjunto de arquivos mais antigo é excluído para liberar espaço para o novo arquivo.

Notas:

- Para comutadores empilhados, você pode coletar dados de serviço do *comutador mestre* e dos *comutadores de espera* com endereços IP que são acessíveis pelo XClarity Administrator. Não é possível coletar dados de serviço de *comutadores membro* ou comutadores que estão no modo protegido.
- Não é possível coletar dados de serviço de comutadores que aceitam o modo de pilha, mas estão no modo independente.

Para obter informações sobre como baixar dados de serviço no XClarity Administrator, consulte Coletando e baixando arquivos de serviço do Lenovo XClarity Administrator.

Para obter informações sobre como enviar dados de serviço manualmente para o Centro de Suporte da Lenovo, consulte Enviando uma solicitação de serviço para problemas de hardware para o Centro de Suporte da Lenovo.

Para obter informações sobre como configurar um encaminhador de serviço automatizado, consulte Configurando uma notificação de problema automática.

Procedimento

Conclua as etapas a seguir para coletar e baixar dados de serviço de um dispositivo gerenciado específico.

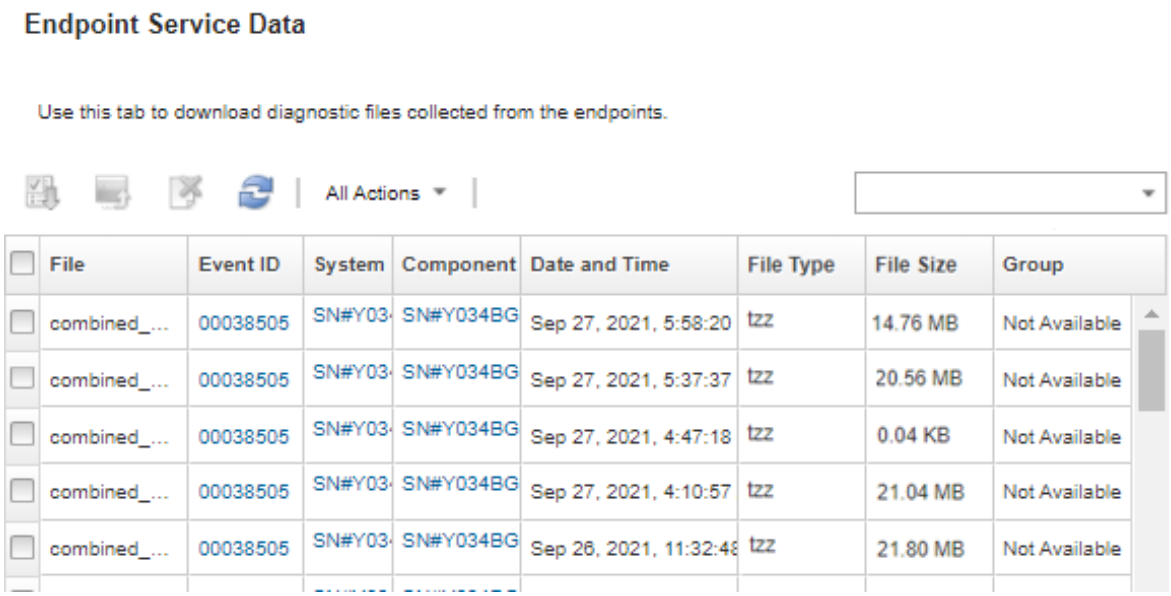
Etapa 1. Na barra de menu do XClarity Administrator, clique em **Administração → Serviço e Suporte**.

Etapa 2. Clique em **Ações de Terminal** na navegação esquerda para exibir a página Ações de Terminal.

Etapa 3. Selecione o dispositivo para o qual você deseja coletar dados de serviço e clique no ícone **Coletar Dados de Serviço** ( ).

Etapa 4. Opcionalmente, salve o arquivo de serviço no sistema local.

Etapa 5. Clique em **Dados de Serviço do Dispositivo** na navegação esquerda para exibir a página Dados de Serviço do Dispositivo. O arquivo de dados de serviço é listado na tabela.



Depois de concluir

Na página Dados de Serviço do Dispositivo, também é possível executar estas tarefas.

- Enviar manualmente arquivos de serviço diretamente a um técnico de serviço Lenovo (consulte Transferindo arquivos de serviço para o Suporte Lenovo).
- Enviar manualmente arquivos de serviço para o Centro de Suporte Lenovo e abrir um tíquete de serviço, consulte Enviando uma solicitação de serviço para problemas de hardware para o Centro de Suporte da Lenovo.
- Anexar arquivos de serviço a um tíquete de serviço existente e enviar para o Centro de Suporte Lenovo selecionando os arquivos e clicando em **Anexar ao Tíquete de Serviço**. Em seguida, selecione o tíquete de serviço e clique em **Associar**.
- Baixar arquivos de serviço selecionando um ou mais arquivos e clicando no ícone **Baixar Arquivos de Serviço Selecionados** ( ). Se vários arquivos forem selecionados, os arquivos serão compactados em um arquivo .tar.gz antes do download.
- Remover arquivos de serviço que não são mais necessários selecionando um ou mais arquivos e clicando no ícone **Excluir Arquivos de Serviço Selecionados** ( ).

Coletando e baixando arquivos de serviço do Lenovo XClarity Administrator

Você pode coletar dados de serviço do Lenovo XClarity Administrator manualmente, especificar dispositivos gerenciados e salvar as informações como um arquivo de serviço no formato tar.gz e baixar ou enviar os arquivos de serviço para seu provedor de serviço preferencial para obter assistência na solução de problemas à medida que ocorrem.

Sobre esta tarefa

Nota: Verifique se você ainda *não* tem um trabalho em andamento para baixar todos os arquivos de serviço (consulte Monitorando trabalhos). Se um usuário iniciou um trabalho que ainda está em andamento, esse mesmo usuário deverá aguardar até que o trabalho seja concluído antes de tentar baixar novamente todos os arquivos de serviço; caso contrário, a segunda tentativa falhará.

Trabalhe com o Suporte da Lenovo para determinar se você deve baixar todos ou alguns arquivos de serviço específicos ou logs.

Até 100 arquivos de serviço para o XClarity Administrator podem ser armazenados no repositório.

Ao baixar os dados de serviço e os logs do XClarity Administrator, você poderá optar por incluir dados de serviço para dispositivos específicos no arquivo baixado. É possível optar por usar arquivos de serviço que já existem ou coletar dados de serviço atuais como parte do processo de download.

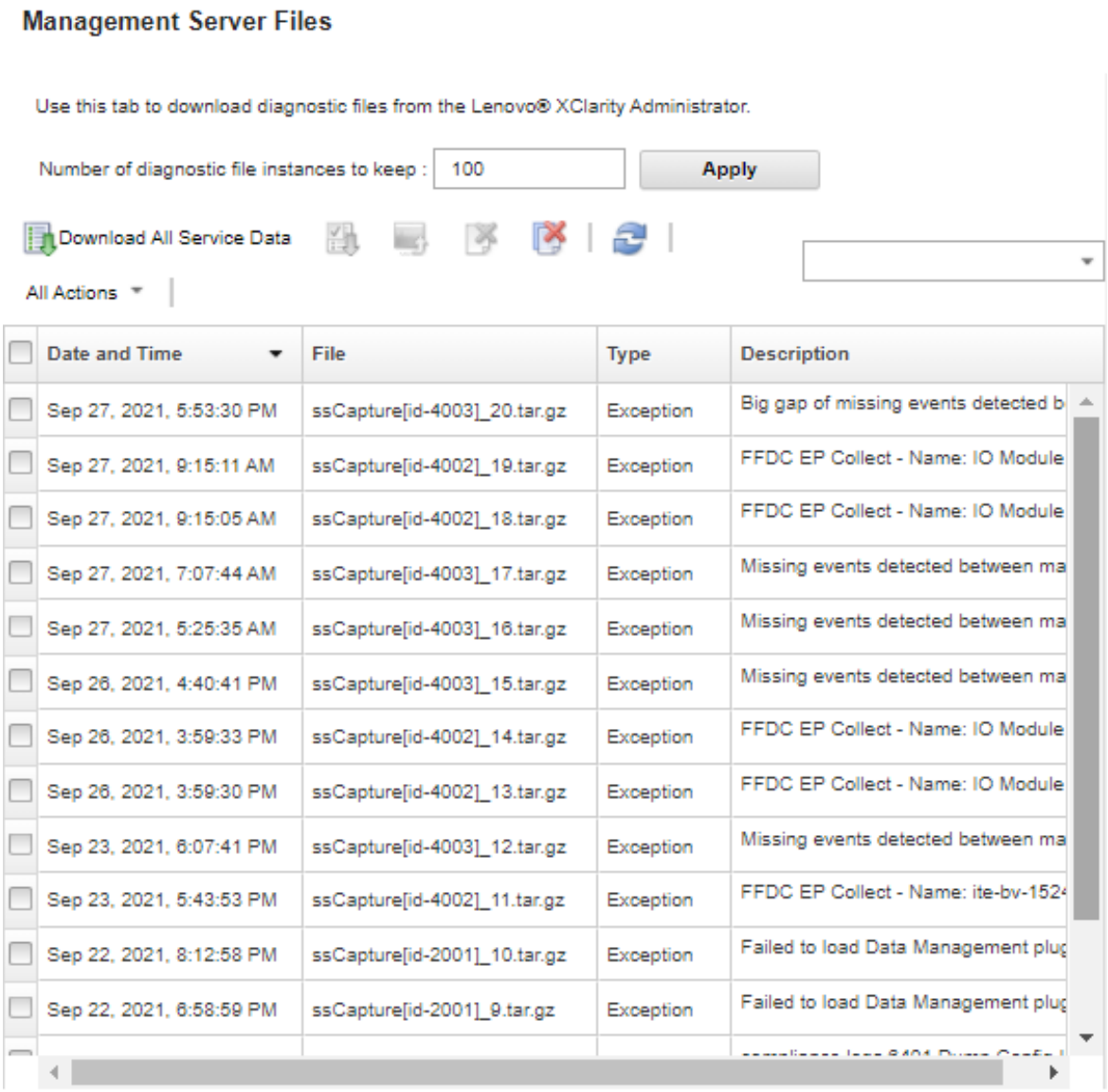
Atenção: Não altere o número de arquivos de serviço a serem mantidos, a menos que seja instruído a fazer isso pelo provedor de serviço.

Procedimento

Para coletar e baixar os dados de serviço ou logs do XClarity Administrator, execute as etapas a seguir.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Administração → Serviço e Suporte**.

Etapa 2. Clique em **Arquivos de Servidor de Gerenciamento** na navegação esquerda para exibir a página Arquivos de Servidor de Gerenciamento.



Etapa 3. Escolha baixar todos os dados de serviço ou todos os logs de serviço.

- Clique em **Baixar Todos os Dados de Serviço** para baixar todos os arquivos de serviço, logs do servidor de gerenciamento e arquivos de serviço de dispositivos específicos.
- Clique em **Todas as Ações → Baixar todos os registros de serviço** para baixar todos os logs do servidor de gerenciamento e arquivos de serviço de dispositivos específicos.

Uma mensagem é exibida mostrando a quantia estimada de dados a serem baixados. Baixar os arquivos de serviço pode levar uma quantidade de tempo significativa, dependendo do número e do tamanho dos arquivos

Etapa 4. Escolha **Incluir dados de serviço que já foram coletados para dispositivos gerenciados**, selecione os arquivos de dados de serviço a serem incluídos e clique em **Aplicar**.

Etapa 5. Escolha **Selecionar os dispositivos gerenciados para os quais você deseja coletar novos dados de serviço**, selecione os dispositivos de destino e clique em **Aplicar**.

Etapa 6. Escolha entre enviar os arquivos de serviço para o Suporte Lenovo ou salvar os arquivos no sistema local ou no armazenamento de rede. Os dados de serviço ou os arquivos de log serão compactados em um único arquivo .tar.gz antes do envio.

- Se você clicar em **Upload da Lenovo**, como opção, insira um número de caso e clique em **OK** para coletar e transferir os arquivos de serviço para o Recurso de Upload da Lenovo.

  Nota: É recomendável fornecer o número de caso para facilitar a localização do arquivo pelo Suporte Lenovo.
- Se você clicar em **Salvar Localmente**, use as funções do seu navegador da Web para salvar o arquivo no sistema local.
- Se você clicar em **Salvar em armazenamento de rede**, especifique o endereço IP, as credenciais, o diretório e a porta e clique em Salvar para transferir os arquivos de serviço para o servidor remoto.

Depois de concluir

Na pagina Arquivos de Servidor de Gerenciamento, também é possível executar estas tarefas:

- Baixe arquivos de serviço existentes selecionando um ou mais arquivos e clicando em **Todas as Ações → Baixar Arquivos de Serviço Selecionados**.

  Você pode optar por enviar os arquivos de serviço para o Suporte Lenovo ou salvar os arquivos no seu sistema local ou no armazenamento de rede. Se vários arquivos forem selecionados, arquivos serão compactados em um único arquivo .tar.gz antes do envio.
- Exclua um ou mais arquivos de serviço selecionados clicando no ícone **Excluir Arquivos de Serviço Selecionados** ( ).
- Exclua todos os arquivos de serviço clicando no ícone **Limpar Todos os Arquivos de Serviço** ( ).
- Exclua todos os logs do servidor de gerenciamento clicando em **Todas as Ações → Limpar Todos os Logs de Serviço**.

Coletando e baixando arquivos de serviço para um Lenovo XClarity Administrator que não responde

Se o Lenovo XClarity Administrator não responder e não for possível recuperá-lo, será possível coletar e baixar dados de serviço e logs para essa instância do XClarity Administrator. Dados de serviço e logs são baixados como um arquivo de serviço em formato tar.gz para seu sistema local

Antes de iniciar

A interface da Web do XClarity Administrator funciona com os navegadores da Web a seguir.
- Chrome™ 48.0 ou posterior (55.0 ou superior para o Console Remoto)
- Firefox® ESR 38.6.0 ou posterior
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 ou posterior (IOS7 ou posterior e OS X)

Faça login na interface da Web de um sistema que tenha conectividade de rede com o sistema no qual o XClarity Administrator está instalado.

Procedimento

Para coletar e baixar os dados de serviço ou logs de uma instância sem resposta do XClarity Administrator, execute as etapas a seguir.

Etapa 1. Aponte seu navegador para o endereço IP da máquina virtual do XClarity Administrator usando o URL a seguir.
`https://<IP_address>:58081`

Exemplo:

`https://192.0.2.0:58081`

Etapa 2. Especifique a senha de recuperação de serviço no campo **passKey**.

Essa é a senha que você especificou ao configurar inicialmente o XClarity Administrator ou alterou a senha na guia **Senha de recuperação do serviço** na página Serviço e Suporte (consulte "Alterando a senha de recuperação de serviço " na página 73).

Etapa 3. Selecione os tipos de arquivos que você deseja coletar.
- **Todos os dados de serviço**. Colete todos os arquivos de serviço e os logs do servidor de gerenciamento.
- **Todos os logs de serviço**. Colete todos os logs do servidor de gerenciamento.

Etapa 4. Clique em **Coletar** e, em seguida, use as funções do seu navegador da Web para salvar o arquivo no sistema local. Os dados de serviço ou os arquivos de log serão compactados em um único arquivo .tar.gz antes do envio.

Enviando uma solicitação de serviço para problemas de hardware para o Centro de Suporte da Lenovo

Se o Call Home for habilitado usando um encaminhador de serviço e ocorrer um evento que permite manutenção em um dispositivo gerenciado, o Lenovo XClarity Administrator abrirá automaticamente um tíquete de serviço, coletará dados de serviço e os salvará como um arquivo. Depois, transferirá o arquivo de serviço para o Recurso de Upload da Lenovo. O arquivo de serviço do arquivo contém os dados de serviço para o dispositivo e para XClarity Administrator. Também é possível coletar e baixar manualmente arquivos de serviço para um dispositivo gerenciado e enviar os arquivos para o Centro de Suporte da Lenovo a qualquer momento usando o XClarity Administrator. Abrir um tíquete de serviço inicia o processo para determinar uma solução para seus problemas de hardware, disponibilizando as informações pertinentes para o Suporte da Lenovo de maneira rápida e eficiente. Os técnicos de serviço do Lenovo poderão começar a trabalhar em sua solução assim que você tiver concluído e aberto um tíquete de serviço.

A Lenovo está comprometida com a segurança. Os dados de serviço que você costuma fazer upload manualmente para o Suporte Lenovo são enviados automaticamente para o Recurso de Upload da Lenovo via HTTPS usando TLS 1.2 ou posterior; seus dados corporativos nunca são transmitidos. O acesso aos dados de serviço no Recurso de Upload da Lenovo é restrito ao pessoal de serviço autorizado.

Antes de iniciar

Atenção: Você deve aceitar a Instrução de privacidade da Lenovo para poder transferir dados para o Suporte Lenovo.

Verifique se as informações de contato de Call Home estão configuradas.

1. Na barra de menu do XClarity Administrator, clique em **Administração → Serviço e Suporte**. A página Serviço e Suporte é exibida.
2. Clique em **Configuração deCall Home** na navegação esquerda para exibir a página Configuração de Call Home.
3. Preencha as informações de contato e local.
4. Opcional: Preencha as informações do sistema.
5. Dê um clique em **Aplicar**.

Verifique se todas as portas que são necessárias para XClarity Administrator (incluindo as portas necessárias para Call Home) estão disponíveis antes de ativar Call Home. Para obter mais informações sobre portas, consulte Disponibilidade de porta na documentação online do XClarity Administrator.

Verifique se existe uma conexão com os endereços da Internet exigidos pelo Call Home. Para obter informações sobre firewalls, consulte Firewalls e servidores proxy na documentação online do XClarity Administrator.

Se o XClarity Administrator acessa a Internet com um proxy HTTP, verifique se o servidor proxy está configurado para usar autenticação básica e configurado como um proxy não encerrando. Para obter mais informações sobre como configurar o proxy, consulte Configurando o acesso à rede na documentação online do XClarity Administrator.

Sobre esta tarefa

Na página Ações de Terminal, a coluna **Status de Call Home** indica se o Call Home está habilitado no Baseboard Management Controller. Um valor "Não Aplicável" indica que o controlador de gerenciamento não oferece suporte ao Call Home. O XClarity Administrator pode executar um Call Home para um dispositivo independentemente do fato de o controlador de gerenciamento oferecer suporte ao Call Home. Para determinar se o Call Home é suportado para um dispositivo específico, consulte a Página da Web Suporte do XClarity Administrator – Compatibilidade.

Para obter mais informações sobre como configurar e ativar Call Home para enviar dados de serviço automaticamente para Centro de Suporte da Lenovo, consulte Configurando a notificação automática do problema para o Suporte Lenovo (Call Home).

Para obter informações adicionais sobre como coletar manualmente e baixar dados de serviço, consulte Coletando e baixando dados de serviço de um dispositivo e Coletando e baixando arquivos de serviço do Lenovo XClarity Administrator.

Procedimento

Conclua as etapas a seguir para abrir um tíquete de serviço manualmente.

- Se Call Home estiver configurado, mas não ativado, execute as seguintes etapas para abrir um tíquete de serviço, coletar e baixar dados de serviço, e enviar os arquivos para o Centro de Suporte da Lenovo:
  1. Na barra de menu do XClarity Administrator, clique em **Administração → Serviço e Suporte**. A página Serviço e Suporte é exibida.
  2. Clique em **Ações de Terminal** na navegação esquerda para exibir a página Ações de Terminal.

3. Selecione o dispositivo e clique em **Todas as Ações → Realizar Manual Call Home**.

   Dica: : É possível testar a comunicação com o Centro de Suporte da Lenovo para verificar se o Call Home está configurado corretamente sem precisar enviar dados para o Suporte da Lenovo clicando em **Todas as Ações → Executar Call Home Testar**.
4. Forneça uma descrição do problema relatado, incluindo IDs relevantes do evento.
5. Clique em **OK**.

- Se Call Home não estiver configurado ou habilitado, será possível enviar uma solicitação de serviço contatando a Suporte Lenovo Line. Para obter mais informações, consulte Obtendo ajuda e assistência técnica .

Depois de concluir

Você pode monitorar tíquetes de serviço abertos na página **Status do Tíquete de Serviço** (consulte Exibindo tíquetes de serviço e o status).

Relatando problemas do XClarity Administrator

Quando você enviar uma solicitação de serviço para relatar problemas de software (servidor de gerenciamento), o Lenovo XClarity Administrator abrirá um tíquete de serviço, coletará dados de serviço do servidor de gerenciamento e enviará os arquivos para o Centro de Suporte Lenovo usando Call Home. A abertura de um tíquete de serviço inicia o processo de determinação de uma solução para seus problemas de software, tornando as informações pertinentes disponíveis para o Suporte da Lenovo de maneira rápida e eficiente. Os técnicos de serviço Lenovo podem começar a trabalhar na sua solução, assim que você tiver concluído e aberto um tíquete de serviço.

A Lenovo está comprometida com a segurança. Os dados de serviço que você costuma fazer upload manualmente para o suporte da Lenovo são enviados automaticamente para o Centro de Suporte da Lenovo via HTTPS usando TLS 1.2 ou posterior; seus dados corporativos nunca são transmitidos. O acesso aos dados de serviço no Centro de Suporte da Lenovo é restrito ao pessoal de serviço autorizado

Antes de iniciar

Atenção: Você deve aceitar a Instrução de privacidade da Lenovo para poder transferir dados para o Suporte Lenovo.

- Antes de enviar uma solicitação de problema para XClarity Administrator, considere encontrar ajuda, usando os seguintes recursos:
  - Envie ideias sobre o XClarity Administrator clicando no menu de ações do usuário (

) na barra de título XClarity Administrator e, em seguida, clicando em **Enviar ideias** ou indo diretamente para o Web site de concepção do Lenovo XClarity.
  - Faça perguntas e encontre respostas clicando no menu de ações do usuário (

) na barra de título XClarity Administrator e, em seguida, clicando em **Visitar fórum** ou indo diretamente para o Site do fórum da comunidade do Lenovo XClarity.
  - Confira o Site de Suporte a data center da Lenovo para obter dicas e técnicas mais recentes que você pode usar para resolver problemas que podem acontecer com o XClarity Administrator. Essas *dicas técnicas* fornecem procedimentos para solucionar problemas relacionados ao funcionamento do XClarity Administrator.

    Para localizar as dicas técnicas disponíveis para seu servidor:

    1. Acesse Site de Suporte a data center da Lenovo.
    2. Insira "XClarity Administrator" no campo **Pesquisar**.

3. Clique em **Exibir Tudo** na seção **Principais Artigos** para exibir todas as dicas ou insira palavras-chave no campo **Pesquisar** para obter uma dica específica.

   Dica: É possível classificar a lista pelas dicas **Relevância**, **Popularidade** ou **Mais novo**.

- Enviar uma solicitação de serviço com o Suporte da Lenovo para problemas no XClarity Administrator requer que o Lenovo XClarity Pro. Lenovo XClarity Pro forneça direito ao serviço e suporte e a licença de ativação com funcionalidade completa. Para obter mais informações sobre a aquisição do Lenovo XClarity Pro, entre em contato com seu representante Lenovo ou o parceiro de negócios autorizado.
- Assegure-se de que o encaminhador de **Call Home da Lenovo padrão** esteja configurado e habilitado (consulte Configurando a notificação automática do problema para o Suporte Lenovo (Call Home)).
- Verifique se todas as portas que são necessárias para o XClarity Administrator (incluindo as portas necessárias para o Call Home) estão disponíveis antes de habilitar o Call Home. Para obter mais informações sobre portas, consulte Disponibilidade de porta na documentação online do XClarity Administrator.
- Verifique se existe uma conexão aos endereços da Internet exigidos pelo Call Home. Para obter informações sobre firewalls, consulte Firewalls e servidores proxy na documentação online do XClarity Administrator.
- Se o XClarity Administrator acessa a Internet com um proxy HTTP, verifique se o servidor proxy está configurado para usar autenticação básica e configurado como um proxy não encerrando. Para obter mais informações sobre como configurar o proxy, consulte Configurando o acesso à rede na documentação online do XClarity Administrator.

Sobre esta tarefa

Se um Call Home já estiver em andamento quando outro Call Home for iniciado, os dados serão coletados e enviados para o Suporte Lenovo para o primeiro Call Home antes de os dados serem coletados e enviados para o segundo Call Home. Portanto, pode haver um atraso no envio de dados para o segundo Call Home.

Procedimento

Conclua as etapas a seguir para relatar um problema com o XClarity Administrator.

- Se o Call Home estiver configurado, execute as etapas a seguir para abrir um tíquete de serviço, coletar e baixar os dados de serviço para o servidor de gerenciamento e enviar os arquivos para o Centro de Suporte Lenovo:
  1. Na barra de título XClarity Administrator, clique em **Relatar Problema**. O servidor de gerenciamento testa a conexão com o Suporte Lenovo.
  2. Clique em **Continuar** para exibir a caixa de diálogo Informações do problema de software.
  3. Forneça o número de cliente Lenovo que você recebeu quando comprou o Lenovo XClarity Pro.
  4. Forneça informações sobre o problema, incluindo os dispositivos e IDs de eventos relevantes associados ao problema.

     Notas:

     – Registros e dados de serviço para o servidor de gerenciamento são coletados e enviados automaticamente.

     – Se você selecionou dispositivos que estão associados com o problema, dados de serviço para os dispositivos também serão coletados e enviados automaticamente.

     – É possível anexar arquivos adicionais para ajudar o Suporte da Lenovo na solução do problema (incluindo capturas de tela e vídeos) clicando em **Fazer upload de arquivo**.
  5. Forneça etapas para reproduzir o problema.

6. Selecione a área funcional na qual ocorreu o problema.
7. Clique em **Avançar**.
8. Especifique as informações sobre a pessoa principal a qual contatar sobre o problema. Para especificar contatos adicionais, clique em **Adicionar Outro Contato**.
9. Clique em **Enviar para a Lenovo** para criar um tíquete de serviço com o Suporte Lenovo.

- Se o Call Home não estiver configurado ou estiver configurado, mas não habilitado, é possível enviar uma solicitação de serviço contatando a Suporte Lenovo Line. Para obter mais informações, consulte Obtendo ajuda e assistência técnica .

Depois de concluir

Você pode monitorar tíquetes de serviço abertos na página **Status do Tíquete de Serviço** (consulte Exibindo tíquetes de serviço e o status).

É possível anexar arquivos adicionais ao tíquete de serviço aberto após o envio do problema.

1. Na barra de menu do XClarity Administrator, clique em **Administração → Serviço e Suporte**. A página Serviço e Suporte é exibida.
2. Clique em **Status do Tíquete de Serviço** na navegação esquerda para exibir a página Status do Tíquete de Serviço.
3. Selecione o tíquete de serviço.
4. Clique em **Anexar Arquivo de Serviço** e, em seguida, selecione o arquivo de dados de serviço ou outro arquivo que deseja anexar ao tíquete de serviço e enviar para o Suporte da Lenovo.

Anexando um arquivo de serviço a um tíquete de serviço aberto

É possível anexar arquivos de dados de serviço para um dispositivo específico a um tíquete de serviço no Centro de Suporte da Lenovo.

Antes de iniciar

Atenção: Você deve aceitar a Instrução de privacidade da Lenovo para poder transferir dados para o Suporte Lenovo.

Sobre esta tarefa

Você pode anexar arquivos adicionais a um tíquete de serviço aberto, como clipes de vídeo, capturas de tela e arquivos de dados de serviço atuais.

Procedimento

Conclua as seguintes etapas para adicionar um arquivo de serviço a um tíquete de serviço aberto.

- Na página **Dados de Serviço do Dispositivo**:
  1. Na barra de menu do Lenovo XClarity Administrator, clique em **Administração → Serviço e Suporte**. A página Serviço e Suporte é exibida.
  2. Clique em **Dados de Serviço do Terminal** na navegação esquerda para exibir a página Dados de Serviço do Terminal.
  3. Selecione um arquivo de serviço que você deseja anexar ao tíquete de serviço.
  4. Clique em **Ações → Anexar ao Tíquete de Serviço** e, em seguida, selecione o tíquete de serviço ao qual deseja anexar o arquivo de serviço.

5. Clique em **Associar** para anexar o arquivo ao tíquete de serviço e enviá-lo ao Suporte Lenovo.

- Na guia **Status do Tíquete de Serviço**:
  1. Na barra de menu do XClarity Administrator, clique em **Administração → Serviço e Suporte**. A página Serviço e Suporte é exibida.
  2. Clique em **Status do Tíquete de Serviço** na navegação esquerda para exibir a página Status do Tíquete de Serviço.
  3. Selecione o tíquete de serviço.
  4. Clique em **Anexar Arquivo de Serviço** e, em seguida, selecione o arquivo de serviço que deseja anexar ao tíquete de serviço e enviar para o Suporte Lenovo.

Exibindo tíquetes de serviço e o status

É possível exibir informações sobre tíquetes de serviço que foram manual e automaticamente enviados para o Centro de Suporte da Lenovo usando Call Home, incluindo o status atual e arquivos de serviço associados que foram transferidos para o Centro de Suporte da Lenovo, e tíquetes de serviço que foram gerados por serviços de suporte diferentes do Call Home.

Procedimento

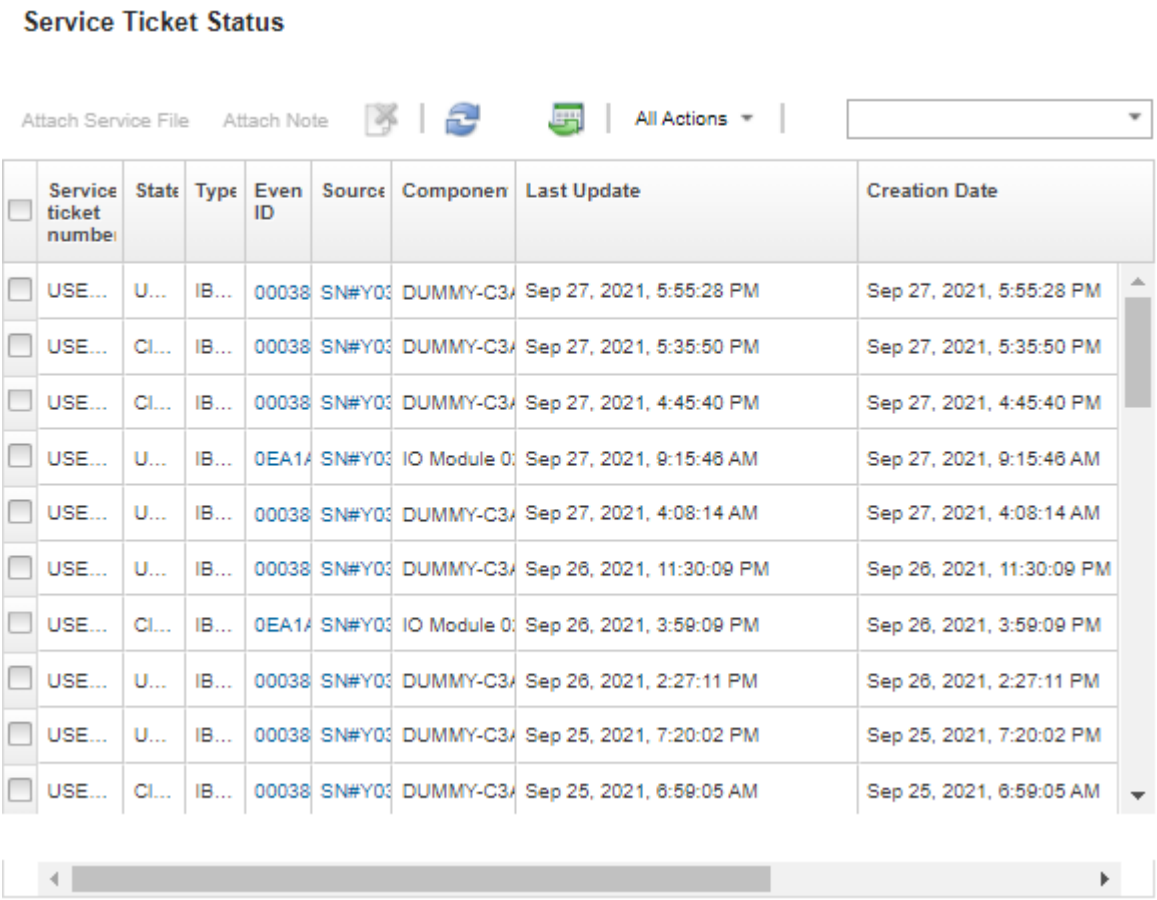
Para exibir tíquetes de serviço no XClarity Administrator, clique em **Administração → Serviço e Suporte** e clique em **Status do Tíquete de Serviço** na navegação esquerda para exibir a página Status do Tíquete de Serviço.

A coluna **Número de ticket de serviço** mostra o ID do tíquete de serviço que foi aberto para um evento. Se vários tíquetes de serviço foram abertos para o mesmo evento (por exemplo, um no Centro de Suporte Lenovo e outro em um integrador ServiceNow), há linhas separadas na tabela para cada tíquete de serviço. Você pode localizar o tíquete de serviço correspondente na coluna **ID de Referência Cruzada**. Por exemplo, se o **Número de Ticket de Serviço** mostrar o ID do tíquete de serviço do Suporte Lenovo, o **ID de Referência Cruzada** mostrará o ID do tíquete de serviço do ServiceNow e vice-versa.

A coluna **Tipo** identifica o tipo de tíquete de serviço que é listado na coluna **Número de ticket de serviço**. O tipo de tíquete de serviço pode ser um dos valores a seguir.
- **Call Home da IBM**
- **Teste de Call Home da IBM**
- **Call Home da Lenovo**
- **Teste de Call Home da Lenovo**
- **Call Home de Software da Lenovo**
- **Teste de Call Home de Software da Lenovo**
- **Cherwill**
- **ServiceNow**

Um tíquete de serviço pode estar em um dos seguintes estados:
- **Ativo**
- **Cancelado**
- **Resolvido**
- **Desconhecido**

A coluna **ID de Referência Cruzada** contém o ID de tíquetes de serviço dos serviços de suporte externos (como ServiceNow) que estão relacionados ao tíquete de serviço Lenovo.



Depois de concluir

Na página Status do Tíquete de Serviço, é possível executar estas etapas em um tíquete de serviço selecionado.

- Conecte um arquivo de serviço para um dispositivo específico a um tíquete de serviço aberto no Centro de Suporte da Lenovo clicando em **Anexar arquivo de serviço**(consulte Anexando um arquivo de serviço a um tíquete de serviço aberto
- Anexe uma nota a um tíquete de serviço aberto no Centro de Suporte da Lenovo clicando em **Anexar Nota**.
- Exclua um tíquete de serviço clicando no ícone **Excluir tíquetes de serviço** ( ). É possível excluir apenas tíquetes de serviço que *não estejam* no estado Ativo.
- Recupere as informações mais recentes sobre todos os tíquetes de serviço abertos no Centro de Suporte da Lenovo clicando no ícone **Atualizar estado de status do tíquete de serviço** ( ).
- Exporte o status de todos os tíquetes de serviço para um arquivo CSV clicando no ícone **Exportar tudo como CSV** ( ).

Transferindo arquivos de serviço para o Suporte Lenovo

Se estiver trabalhando com o Suporte Lenovo para solucionar um problema, você poderá transferir manualmente arquivos de serviço diretamente ao representante do Suporte Lenovo utilizando o Recurso de Upload da Lenovo.

Antes de iniciar

Atenção: Você deve aceitar a Instrução de privacidade da Lenovo para poder transferir dados para o Suporte Lenovo.

Procedimento

Conclua as seguintes etapas para transferir arquivos de serviço diretamente ao Suporte Lenovo.

Etapa 1. Configure o Recurso de Upload da Lenovo.

a. Na barra de menu do Lenovo XClarity Administrator, clique em **Administração → Serviço e Suporte**. A página Serviço e Suporte é exibida.

b. Clique em **Recurso de Upload da Lenovo** na navegação esquerda.

c. Insira um endereço de e-mail.

d. Clique em **Aplicar**.

Etapa 2. Clique em **Arquivos de Servidor de Gerenciamento** ou **Dados de Serviço do Terminal** na navegação esquerda, dependendo dos logs que você precisa enviar.

Etapa 3. Selecione um ou mais arquivos de serviço que deseja enviar para o Suporte Lenovo e clique no ícone **Upload da Lenovo Selecionado** ( ). A caixa de diálogo Informações de Upload da Lenovo é exibida.

Etapa 4. Opcionalmente, insira um número de caso.

Etapa 5. Clique em **OK** para transferir os arquivos de serviço.

Definindo configurações de log do servidor de gerenciamento

As configurações do log são usadas pelo Suporte da Lenovo para ajustar a granularidade do log apenas quando necessário.

Sobre esta tarefa

Atenção: Não altere as configurações nesta página, a menos que seja instruído a fazer isso pelo Suporte da Lenovo.

Procedimento

Conclua as etapas a seguir para definir as configurações de log.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Administração → Serviço e Suporte**. A página Serviço e Suporte é exibida.

Etapa 2. Clique em **Configurações de Criação de Log de Servidor** na navegação esquerda para exibir a página Configurações de Criação de Log de Servidor.

Etapa 3. Ajuste cada configuração conforme instruído pelo Suporte da Lenovo e clique em **Aplicar**.

Depois de concluir

Na página Configurações de Criação de Log de Servidor, também é possível executar as etapas a seguir.

- Baixe as definições de configuração de log de servidor de gerenciamento para o sistema local clicando em **Baixar LogBack**. As configurações são baixadas para o diretório de download padrão como um arquivo denominado logback.xml.
- Clique em **Restaurar Padrões** para restaurar as configurações padrão.
- Importar um arquivo de configuração clicando em **Fazer Upload do Arquivo de Configuração** e selecionando o arquivo que deseja importar no XClarity Administrator. O arquivo deve ser denominado logback.xml.

Importante: Apenas os arquivos de configuração que foram fornecidos pelo técnico de serviço da Lenovo devem ser importados e somente mediante solicitação do técnico de serviço.

Reativando Call Home em todos os dispositivos gerenciados

Quando você habilita um encaminhador de serviços Call Home no Lenovo XClarity Administrator, o Call Home é desabilitado em todos os dispositivos gerenciados para evitar a criação de registros de problema duplicados. Se você pretende deixar de usar o XClarity Administrator para gerenciar dispositivos ou se pretende desativar Call Home em XClarity Administrator, poderá reativar Call Home em todos os dispositivos gerenciados no XClarity Administrator em vez de reativar Call Home para cada dispositivo individual posteriormente.

Sobre esta tarefa

Atenção: A reativação de Call Home em todos os dispositivos pode fazer com que o Call Home não funcione nesses dispositivos. A configuração pode ser necessária em cada dispositivo individual, caso não tenha sido configurada nesses dispositivos antes.

Embora o XClarity Administrator ofereça suporte ao Call Home para dispositivos ThinkAgile e ThinkSystem, o Baseboard Management Controller para alguns dispositivos ThinkAgile e ThinkSystem não inclui suporte a Call Home. Portanto, não é possível ativar ou desativar o Call Home nesses dispositivos. O Call Home só pode ser habilitado para esses dispositivos no nível do XClarity Administrator.

Procedimento

Conclua as seguintes etapas para reativar Call Home em todos os dispositivos gerenciados.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Administração → Serviço e Suporte**. A página Serviço e Suporte é exibida.

Etapa 2. Clique em **Encaminhadores de Serviços** na navegação esquerda para exibir a página Encaminhadores de Serviços.

Etapa 3. Altere o status de todos os encaminhadores de serviço de Call Home, incluindo o "Call Home Padrão", para **Desabilitado**.

Etapa 4. Clique em **Ações de Terminal** na navegação esquerda para exibir a página Ações de Terminal.

Etapa 5. Clique em **Todas as Ações → Ativar Call Home em todos os dispositivos** para ativar Call Home em cada dispositivo gerenciado.

Enviando dados periódicos à Lenovo

Se desejar, é possível permitir que o XClarity Administrator colete informações sobre como usar o produto e as alterações em seu ambiente e enviar esses dados para a Lenovo periodicamente. A Lenovo usa esses dados para melhorar sua experiência com os produtos da Lenovo e com o Suporte Lenovo.

Antes de iniciar

Atenção: Você deve aceitar a Instrução de privacidade da Lenovo para poder transferir dados para o Suporte Lenovo.

Sobre esta tarefa

É possível coletar e enviar os seguintes tipos de dados para a Lenovo.

- **Dados de uso**

Analisando dados de uso de vários usuários, a Lenovo pode saber mais sobre como o XClarity Administrator está sendo usado. Isso permite que a Lenovo conheça as funções usadas e identifique os problemas que estão ocorrendo nas instâncias do XClarity Administrator. Esses dados podem ser usados para tomar decisões futuras sobre investimentos em aprimoramentos de produtos que atendam melhor às suas necessidades, corrigir problemas em versões futuras e melhorar a qualidade do produto.

Quando você concorda em enviar dados de uso para a Lenovo, os dados a seguir são coletados e enviados semanalmente. Esses dados *são anônimos*. Nenhum dado privado (incluindo números de série, UUIDs, nomes de host, endereços IP e nomes de usuário) é coletado ou enviado para a Lenovo.
- Log de ações executadas
- Lista de eventos que foram gerados e o carimbo de data e hora em que foram gerados
- Lista de eventos de auditoria que foram gerados e o carimbo de data e hora em que foram gerados
- Lista de trabalhos que foram executados e informações de êxito ou falha para cada trabalho
- Métricas do XClarity Administrator, incluindo uso da memória, uso do processador e espaço em disco
- Dados do inventário limitados sobre todos os dispositivos gerenciados

- **Dados de hardware**

  Analisando dados de hardware de vários usuários, a Lenovo pode saber mais sobre alterações de hardware que ocorrem regularmente. Esses dados podem ser usados para melhorar a análise de previsão e aprimorar sua experiência de serviço e suporte, estocando peças nas regiões corretas.

  Quando você concorda em enviar dados de hardware para a Lenovo, os dados a seguir são coletados e enviados periodicamente. Esses dados *não são anônimos*. Os dados de hardware incluem atributos, como UUIDs e números de série. Não incluem endereços IP ou nomes de host.

  - **Dados de hardware diários**. Os dados a seguir são incluídos para cada alteração de inventário.
    - Evento de alteração de inventário (FQXHMDM0001I)
    - Alterações nos dados de inventário do dispositivo associado a esse evento
  - **Dados de hardware semanais**. Os dados do inventário são incluídos para todos os dispositivos gerenciados.

Quando os dados são enviados para a Lenovo, eles são transmitidos da instância do XClarity Administrator para o Recurso de Upload da Lenovo usando HTTPS. As APIs REST são chamadas sobre essa conexão HTTPS para enviar os dados. Um certificado pré-carregado no XClarity Administrator é usado para autenticação. Se uma instância do XClarity Administrator não tiver acesso direto à Internet e houver um proxy configurado no XClarity Administrator, os dados serão transmitidos por esse proxy.

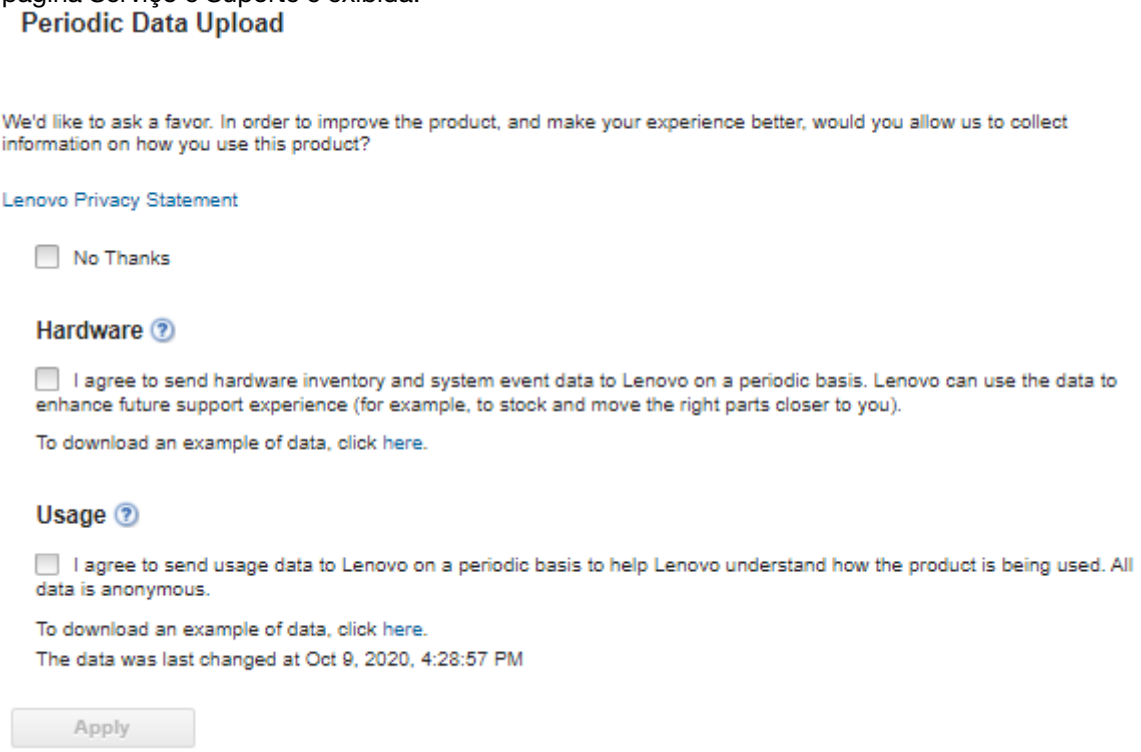
Em seguida, os dados são movidos para o repositório Lenovo Customer Care, onde são armazenados por até 5 anos. Esse repositório é um local seguro que também é usado quando os dados de depuração são enviados para a Lenovo para solucionar problemas. Ele é usado pela maioria dos produtos de servidor, armazenamento e comutador da Lenovo.

No repositório Lenovo Customer Care, as consultas são executadas em todos os dados de hardware e de uso, e os gráficos são disponibilizados para a equipe de produtos da Lenovo para análise.

Procedimento

Conclua as etapas a seguir para permitir que o XClarity Administrator colete e envie dados do cliente para a Lenovo.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Administração → Serviço e Suporte**. A página Serviço e Suporte é exibida.



Etapa 2. Clique em **Upload de Dados Periódico** na navegação esquerda para exibir a página Upload de Dados Periódico

Etapa 3. Se desejar, concorde em enviar dados de hardware e uso para a Lenovo

Etapa 4. Clique em **Aplicar**.

Depois de concluir

É possível executar as seguintes ações nesta página se você tiver concordado em enviar dados.

- Determine a última vez em que os dados foram enviados olhando a data na caixa de seleção apropriada.
- Baixe o arquivo de dados enviado pela última vez clicando no link na caixa de seleção apropriada.

Dados de uso de amostra

Os exemplos a seguir são coletados e enviados para a Lenovo periodicamente quando você concorda em enviar dados de uso para a Lenovo.

Dados métricos do XClarity Administrator

```
Timestamp   cpuLoad  usedSpace  usedRam  usedJavaCpu  usedJavaRam
1497861662  0.99     12.6225    13.3644  71.9          9.4
1497861668  1.23     12.6343    18.5676  0             14.4
1497861674  1.89     12.6371    19.6182  77.9         15.3
1497861679  1.98     12.6442    23.0782  37.9         18.6
1497861685  2.06     12.647     23.2412  77.9         18.6
1497861690  2.14     12.6654    25.3697  10            19
1497861696  2.37     7.75276    25.8952  2             19.4
1497861701  2.34     7.76077    26.0184  24            19.5
1497861056  2.55     7.77003    26.4222  85.9         19.7
1497861061  2.82     7.77877    26.5485  159.9        19.7
1497861067  3         7.7954     27.0066  131.9        20
```

Dados de ações


```
/updates/images/userdefined.png={"GET"\:1}
/config/profile={"GET"\:865}
/node/AD9547AB3C8011E79DCC000E1E7D4EE0={"GET"\:1}
/usage/data={"GET"\:12}
/compliancePolicies/persistedResult={"GET"\:3}
/jobs/88={"PUT"\:31}
/osdeployment/rest/internal/event/aicc={"POST"\:186}
/aicc={"GET"\:56}
/updates/images/powerStates.png={"GET"\:2}
/jobs/84={"PUT"\:3}
/updates/images/ActionSprite.png={"GET"\:1}
/nodes/AD9547AB3C8011E79DCC000E1E7D4EE0/lock={"GET"\:1,"PUT"\:2}
/updates/customUI/gridxExtensions/Mark.js={"GET"\:2}
/updates/images/ac22_deleteall_inactive_24.png={"GET"\:1}
/service/forwarders={"GET"\:12}
/nodes/7C64A0A8413811E7A6C6000E1EB35A90/lock={"GET"\:1,"PUT"\:2}
/config/deploy/status={"GET"\:865}
/node/235435543C7D11E7AA13000E1E7D54A0={"GET"\:1}
/updates/ApplyActivateUpdates.js={"GET"\:2}
/discovery={"GET"\:3}
/userAccountSettings={"GET"\:1}
/discoverRequest/jobs/610={"GET"\:9}
/compliancePolicies/events={"POST"\:25}
/events/audit={"GET"\:5}
/updates/images/st22_filterRunning_24.png={"GET"\:2}
/updates/images/st16_running_24.gif={"GET"\:1}
/updates/images/complianceStatus.png={"GET"\:2}
/usage={"GET"\:4}
/updates/json/firmwareRepository/exportPayloads.json={"GET"\:1}
/updates/images/ac22_collapseall_OneUI_24.png={"GET"\:3}
/chassis/0AC502DEFCD6419FB20FB5A9A49D0293={"GET"\:17}
/updates/images/ac22_copy_inactive_24.png={"GET"\:1}
/service/endPoint/collectedArchives={"GET"\:4}
/jobs/lock/88={"DELETE"\:1}
/updates/customUI/gridxModules/IndirectSelect.js={"GET"\:2}
/stgupdates/inventory/events={"POST"\:70}
/electronicDownload={"GET"\:1}
/updates/images/st16_firm_normal_24.png={"GET"\:3}
/updates/images/st16_Empty_24.png={"GET"\:1}
/updates/json/compliancePolicy/getCompByUxsp.json={"GET"\:1}
```


Dados do evento


```
{
   "action":100,
   "commonEventID":"FQXHMSE0203I",
   "cn":"1",
   "eventClass":200,
   "eventID":"FQXHMSE0203I",
   "flags":"",
   "mtm":"",
   "msgID":"",
   "service":100,
   "severity":200},
   "timeStamp":"2017-06-16T15:56:06Z"
}
```


Dados de auditoria


```
{
```

```
   "action":100,
   "commonEventID":"FQXHMSE0200I",
   "cn":"1",
   "eventClass":200,
   "eventID":"FQXHMSE0200I",
   "flags":"",
   "msgID":"",
   "mtm":"",
   "service":100,
   "severity":200,
   "timeStamp":"2017-06-16T15:56:06Z"
}
```


Dados do inventário


```
-377665639={
   "firmwareList"\:[{
      "build"\:"2PET41C",
      "date"\:"2017-12-19T05\:00\:00Z",
      "name"\:"CMM firmware",
      "type"\:"CMM firmware",
      "version"\:""
   }],
   "mtm"\:"/",
   "productName"\:"",
   "stillManaged"\:"true",
   "uuid"\:"-377665639"
}
-177044123={
   "firmwareList"\:[{
      "build"\:"A3E117D",
      "date"\:"2018-01-26T00\:00\:00Z",
      "name"\:"UEFI Firmware/BIOS",
      "type"\:"UEFI",
      "version"\:"A3E117D-1.80"
   },{
      "build"\:"A3E113C",
      "date"\:"2016-12-16T00\:00\:00Z",
      "name"\:"UEFI Backup Firmware/BIOS",
      "type"\:"UEFI-Backup",
      "version"\:"A3E113C-1.60"
   },{
      "build"\:"DSALB1Q",
      "date"\:"2018-05-15T00\:00\:00Z",
      "name"\:"DSA Diagnostic Software",
      "type"\:"DSA",
      "version"\:"DSALB1Q-10.3"
   },{
      "build"\:"TCOO39A",
      "date"\:"2018-01-19T00\:00\:00Z",
      "name"\:"IMM2 Firmware",
      "type"\:"IMM2",
      "version"\:"TCOO39A-4.70"
   },{
      "build"\:"TCOO39A",
      "date"\:"2018-01-19T00\:00\:00Z",
      "name"\:"IMM2 Backup Firmware",
      "type"\:"IMM2-Backup",
      "version"\:"TCOO39A-4.70"
   }],
   "mtm"\:"7162/CC1",
```

```
   "productName"\:"Lenovo Flex System x240 Compute Node",
   "stillManaged"\:"true",
   "uuid"\:"-177044123"
}
-734000615={
   "firmwareList"\:[],
   "mtm"\:"8721/HC1",
   "productName"\:"IBM Flex System Enterprise Chassis Midplane Card"},
   "stillManaged"\:"true",
   "uuid"\:"-734000615"
1150304995={
   "firmwareList"\:[{
      "date"\:"06/12/2014",
      "build"\:"",
      "name"\:"Boot ROM",
      "type"\:"Boot ROM",
      "version"\:"7.8.5.0"
   },{
      "date"\:"06/12/2014",
      "build"\:"",
      "name"\:"Main Application 1",
      "type"\:"Main Application 1",
      "version"\:"7.8.5.0"
   },{
      "date"\:"03/29/2013",
      "build"\:"",
      "name"\:"Main Application 2",
      "type"\:"Main Application 2",
      "version"\:"7.5.3.0"
   }],
   "mtm"\:"/",
   "productName"\:"IBM Flex System Fabric EN4093 10Gb Scalable Switch",
   "stillManaged"\:"true",
   "uuid"\:"1150304995"
}
-1050714125={
   "firmwareList"\:[{
      "date"\:"04/19/2016",
      "build"\:"",
      "name"\:"Main Application",
      "type"\:"Main Application",
      "version"\:"7.4.1c"
   }],
   "mtm"\:"/",
   "productName"\:"IBM Flex System FC5022 12-port 16Gb ESB SAN Scalable Switch",
   "stillManaged"\:"true",
   "uuid"\:"-1050714125"
}
```


Dados de hardware de amostra

O exemplo a seguir é coletado e enviado à Lenovo periodicamente quando você concorda em enviar dados de hardware para a Lenovo.

Os dados são coletados diária e semanalmente.

- "Dados de hardware diários" na página 93. Inclui o evento de alteração de inventário (FQXHMDM0001I) e as alterações no inventário de hardware para cada alteração de inventário.
- "Dados de hardware semanais" na página 97. Inclui o inventário de todos os dispositivos.

Dados de hardware diários


```
[{
   "2020-03-23T12:32:24.765": {
      "event": {
         "severity": 200,
         "timeStamp": "2020-03-23T16:32:21Z",
         "eventID": "FQXHMDM0001I",
         "eventClass": 800,
         "service": 100,
         "mtm": "",
         "flags": ["Hidden"],
         "action": 100,
         "msgID": "",
         "commonEventID": "FQXHMDM0001I",
         "cn": ""
      },
      "deviceInventoryChanges": [{
         "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36": [{
            "MODIFIED": [
               { "nodes": [] },
               { "accessState": "Pending" },
               { "powerSupplies": [{
                  "cmmDisplayName": "Power Supply 06",
                  "cmmHealthState": "Non-Critical",
                  "dataHandle": 0,
                  "description": "Power Supply",
                  "excludedHealthState": "Normal",
                  "firmware": [{
                     "build": "",
                     "classifications": [],
                     "date": "",
                     "name": "Power Supply Firmware",
                     "revision": "0",
                     "role": "",
                     "softwareID": "",
                     "status": "",
                     "type": "Power Supply Firmware",
                     "version": ""
                  }],
                  "FRU": "69Y5817",
                  "fruSerialNumber": "ZK125115V0VS",
                  "hardwareRevision": "5.0",
                  "healthState": "NA",
                  "inputVoltageMax": -1,
                  "inputVoltageIsAC": true,
                  "inputVoltageMin": -1,
                  "leds": [{
                     "color": "Green",
                     "location": "Planar",
                     "name": "OUT",
                     "state": "Off"
                  },
                  {
                     "color": "Amber",
                     "location": "Planar",
                     "name": "FAULT",
                     "state": "Off"
                  },
                  {
                     "color": "Green",
```

```
            "location": "Planar",
            "name": "IN",
            "state": "Off"
        }],
        "machineType": "",
        "manufactureDate": "2211",
        "manufacturer": "IBM",
        "manufacturerId": "20301",
        "model": "",
        "name": "Power Supply 06",
        "overallHealthState": "Normal",
        "parent": {
            "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
            "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
        },
        "partNumber": "69Y5801",
        "productName": "IBM 2500 W Power Supply",
        "posID": "60",
        "powerAllocation": {
            "totalInputPower": 0,
            "totalOutputPower": 343
        },
        "powerState": "Unknown",
        "productId": "303",
        "serialNumber": "",
        "slots": [6],
        "type": "PowerSupply",
        "userDescription": "",
        "uri": "powerSupply/04382F96885411E00095009500950095",
        "uuid": "04382F96885411E00095009500950095",
        "vpdID": "128"
    },
    {
        "cmmDisplayName": "Power Supply 04",
        "cmmHealthState": "Normal",
        "dataHandle": 0,
        "description": "Power Supply",
        "excludedHealthState": "Normal",
        "firmware": [{
            "build": "",
            "classifications": [],
            "date": "",
            "name": "Power Supply Firmware",
            "revision": "5",
            "role": "",
            "softwareID": "",
            "status": "",
            "type": "Power Supply Firmware",
            "version": ""
        }],
        "FRU": "69Y5806",
        "fruSerialNumber": "ZK128116T03B",
        "hardwareRevision": "75.54",
        "healthState": "NA",
        "inputVoltageIsAC": true,
        "inputVoltageMax": 240,
        "inputVoltageMin": 220,
        "leds": [{
            "color": "Green",
            "location": "Planar",
            "name": "OUT",
```

```
            "state": "On"
        },
        {
            "color": "Amber",
            "location": "Planar",
            "name": "FAULT",
            "state": "Off"
        },
        {
            "color": "Green",
            "location": "Planar",
            "name": "IN",
            "state": "On"
        }],
        "machineType": "",
        "manufactureDate": "2511",
        "manufacturer": "IBM",
        "manufacturerId": "20301",
        "model": "",
        "name": "Power Supply 04",
        "overallHealthState": "Normal",
        "parent": {
            "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
            "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
        },
        "partNumber": "69Y5802",
        "productId": "304",
        "productName": "IBM 2500 W Power Supply",
        "powerAllocation": {
            "totalInputPower": 2505,
            "totalOutputPower": 343
        },
        "powerState": "Unknown",
        "posID": "61",
        "serialNumber": "",
        "slots": [4],
        "type": "PowerSupply",
        "userDescription": "",
        "uri": "powerSupply/FF2D840D7A644BCE91ADC16C78978A03",
        "uuid": "FF2D840D7A644BCE91ADC16C78978A03",
        "vpdID": "128"
    }]},
    { "fanMuxes": [{
        "cmmDisplayName": "Fan Logic 01",
        "cmmHealthState": "Non-Critical",
        "dataHandle": 0,
        "description": "Fan Logic Module",
        "excludedHealthState": "Normal",
        "FRU": "81Y2912",
        "fruSerialNumber": "Y031BG16D00S",
        "hardwareRevision": "4.0",
        "leds": [{
            "color": "Amber",
            "location": "FrontPanel",
            "name": "FAULT",
            "state": "On"
        }],
        "machineType": "",
        "manufacturer": "IBM",
        "manufactureDate": "2511",
        "manufacturerId": "20301",
```

```
                "model": "",
                "name": "Fan Logic 01",
                "overallHealthState": "Normal",
                "parent": {
                   "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
                   "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
                },
                "partNumber": "81Y2990",
                "productId": "338",
                "productName": "IBM Fan Pack Multiplexor Card",
                "status": "Non-Critical",
                "serialNumber": "",
                "slots": [1],
                "type": "FanMux",
                "uri": "fanMux/4247F859984711E08372E99E4175BAB0",
                "uuid": "4247F859984711E08372E99E4175BAB0"
             },
             {
                "cmmDisplayName": "Fan Logic 02",
                "cmmHealthState": "Non-Critical",
                "dataHandle": 0,
                "description": "Fan Logic Module",
                "excludedHealthState": "Normal",
                "FRU": "81Y2912",
                "fruSerialNumber": "Y031BG16D0CE",
                "hardwareRevision": "4.0",
                "leds": [{
                   "color": "Amber",
                   "location": "FrontPanel",
                   "name": "FAULT",
                   "state": "On"
                }],
                "machineType": "",
                "manufactureDate": "2511",
                "manufacturer": "IBM",
                "manufacturerId": "20301",
                "model": "",
                "name": "Fan Logic 02",
                "overallHealthState": "Normal",
                "parent": {
                   "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
                   "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
                },
                "productId": "338",
                "productName": "IBM Fan Pack Multiplexor Card",
                "partNumber": "81Y2990",
                "serialNumber": "",
                "slots": [2],
                "status": "Non-Critical",
                "type": "FanMux",
                "uri": "fanMux/71F72BE3985011E0B5A8E216694D6175",
                "uuid": "71F72BE3985011E0B5A8E216694D6175"
             }]},
             { "switches": [] },
             { "excludedHealthState": "Normal" },
             { "overallHealthState": "Normal" },
             { "inventoryState": null }
          ]}
       ]
    }]
}
```

```
}]
```


Dados de hardware semanais


```
{
   "2020-03-23T12:41:28.045": {
      "cabinetList": [{
         "cabinetName": "STANDALONE_OBJECT_NAME",
         "chassisList": [{
            "itemName": "SN#Y010BG57Y01G",
            "itemUUID": "671D5D9EBB4440A49D9DAF08A9EDFB36",
            "itemParentUUID": "",
            "itemLocationRoom": "",
            "itemLocationRack": "",
            "itemLocation": "No Location ConfiguredL",
            "itemLowerUnit": 0,
            "itemType": "CHASSIS",
            "itemHeight": 10,
            "itemSubType": "unknown_type",
            "itemInventory": {
               "accessState": "Online",
               "activationKeys": [],
               "backedBy": "real",
               "bladeSlots": 14,
               "cmmDisplayName": "SN#Y010BG57Y01G",
               "cmmHealthState": "Non-Critical",
               "cmms": [{
                  "accessState": "Online",
                  "backedBy": "real",
                  "cmmDisplayName": "Standby CMM",
                  "dataHandle": 1584981183026,
                  "cmmHealthState": "Normal",
                  "description": "CMM",
                  "firmware": [{
                     "build": "1AON58O",
                     "classifications": [],
                     "date": "2020-03-20T04:00:00Z",
                     "name": "CMM firmware",
                     "revision": "58",
                     "role": "",
                     "status": "",
                     "type": "CMM firmware",
                     "version": "2.5.0"
                  }],
                  "FRU": "68Y7032",
                  "fruSerialNumber": "Y030BG168020",
                  "hostConfig": [],
                  "ipInterfaces": [{
                     "IPv4DHCPmode": "UNKNOWN",
                     "IPv4enabled": false,
                     "IPv6DHCPenabled": false,
                     "IPv6enabled": false,
                     "IPv6statelessEnabled": false,
                     "IPv6staticEnabled": false,
                     "label": "External",
                     "name": "eth0"
                  }],
                  "errorFields": [],
                  "excludedHealthState": "Normal",
                  "leds": [{
                     "color": "Amber",
```

```
        "location": "FrontPanel",
        "name": "FAULT",
        "state": "Off"
     }],
     "machineType": "",
     "manufacturer": "IBM",
     "manufacturerId": "20301",
     "model": "",
     "name": "Standby CMM",
     "overallHealthState": "Normal",
     "partNumber": "68Y7054",
     "parent": {
        "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
        "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36"
     },
     "powerAllocation": {
        "maximumAllocatedPower": 20,
        "minimumAllocatedPower": 20
     },
     "productId": "65",
     "role": "backup",
     "serialNumber": "",
     "slots": [2],
     "type": "CMM",
     "uri": "cmm/F1F06BE6946511E089AEB9871E6892B2",
     "userDefinedName": "",
     "userDescription": "",
     "uuid": "F1F06BE6946511E089AEB9871E6892B2"
  }],
  "complex": [],
  "contact": "No Contact Configured",
  "dataHandle": 1584981227532,
  "description": "Lenovo Flex System Chassis",
  "displayName": "SN#Y010BG57Y01G",
  "encapsulation": {
     "encapsulationMode": "normal"
  },
  "energyPolicies": {
     "acousticAttenuationMode": "Off",
     "hotAirRecirculation": {
        "chassisBay": [],
        "isEnabled": false,
        "maxVariation": 9.0
     },
     "powerCappingPolicy": {
        "cappingPolicy": "OFF",
        "currentPowerCap": 0,
        "maxPowerCap": 5010,
        "minPowerCap": 1504,
        "powerCappingAllocUnit": "watts"
     },
     "powerRedundancyMode": 4
  },
  "errorFields": [],
  "excludedHealthState": "Warning",
  "fanSlots": 10,
  "fanMuxes": [{
     "cmmDisplayName": "Fan Logic 02",
     "cmmHealthState": "Non-Critical",
     "dataHandle": 0,
     "description": "Fan Logic Module",
```

```
      "excludedHealthState": "Warning",
      "FRU": "81Y2912",
      "fruSerialNumber": "Y031BG16D0CE",
      "hardwareRevision": "4.0",
      "leds": [{
         "color": "Amber",
         "location": "FrontPanel",
         "name": "FAULT",
         "state": "On"
      }],
      "machineType": "",
      "manufactureDate": "2511",
      "manufacturer": "IBM",
      "manufacturerId": "20301",
      "model": "",
      "name": "Fan Logic 02",
      "overallHealthState": "Warning",
      "parent": {
         "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
         "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36"
      },
      "partNumber": "81Y2990",
      "productId": "338",
      "productName": "IBM Fan Pack Multiplexor Card",
      "serialNumber": "",
      "slots": [2],
      "status": "Non-Critical",
      "type": "FanMux",
      "uri": "fanMux/71F72BE3985011E0B5A8E216694D6175",
      "uuid": "71F72BE3985011E0B5A8E216694D6175"
   }],
   "fanMuxSlots": 2,
   "fans": [{
      "cmmDisplayName": "Fan 06",
      "cmmHealthState": "Normal",
      "dataHandle": 0,
      "description": "IBM Fan Pack",
      "errorFields": [],
      "excludedHealthState": "Normal",
      "firmware": [{
         "build": "",
         "classifications": [],
         "date": "",
         "name": "Fan Controller",
         "revision": "226",
         "role": "",
         "status": "",
         "type": "Fan Controller",
         "version": "226"
      }],
      "FRU": "88Y6685",
      "fruSerialNumber": "YK10JPB69582",
      "hardwareRevision": "4.0",
      "leds": [{
         "color": "Amber",
         "location": "FrontPanel",
         "name": "FAULT",
         "state": "Off"
      }],
      "machineType": "",
      "manufactureDate": "2411",
```

```
      "manufacturer": "IBM",
      "manufacturerId": "20301",
      "model": "",
      "name": "Fan 06",
      "overallHealthState": "Normal",
      "parent": {
         "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
         "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36"
      },
      "partNumber": "88Y6691",
      "posID": "11",
      "powerAllocation": {
         "maximumAllocatedPower": 75,
         "minimumAllocatedPower": 75
      },
      "powerState": "Unknown",
      "productId": "342",
      "productName": "80mm Fan Pack for ITE Cooling",
      "serialNumber": "",
      "slots": [6],
      "type": "Fan",
      "userDescription": "",
      "uri": "fan/7293CA21938011E0BC13CB5D330B7C19",
      "uuid": "7293CA21938011E0BC13CB5D330B7C19",
      "vpdID": "373"
   }],
   "height": 10,
   "isConnectionTrusted": "true",
   "lastOfflineTimestamp": -1,
   "ledCardSlots": 1,
   "leds": [{
      "color": "Blue",
      "location": "FrontPanel",
      "name": "Location",
   "state": "Off"
   }],
   "location": {
      "location": "No Location ConfiguredL",
      "lowestRackUnit": 0,
      "rack": "",
      "room": ""
   },
   "machineType": "8721",
   "managerName": "UNKNOWN",
   "managerUuid": "UNKNOWN",
   "manufacturer": "IBM",
   "manufacturerId": "20301",
   "mmSlots": 2,
   "model": "HC1",
   "name": "SN#Y010BG57Y01G",
   "nist": {
      "currentValue": "Compatibility",
      "possibleValues": ["Nist_800_131A_Strict","unsupported","Nist_800_131A_Custom","Compatibility"]
   },
   "nodes": [{
      "accessState": "Online",
      "activationKeys": [],
      "addinCards": [],
      "addinCardSlots": 0,
      "arch": "Unknown",
      "backedBy": "real",
```

```
"bladeState": 0,
"bladeState_health": "CRITICAL",
"bladeState_string": "Init failed",
"bootMode": {
   "currentValue": "",
   "possibleValues": []
},
"bootOrder": {
   "bootOrderList": [],
   "uri": "nodes/DUMMY-671D5D9EBB4440A4-CHASSIS(1)-BLADE(7)/bootOrder"
},
"cmmDisplayName": "Node 07",
"cmmHealthState": "Critical",
"complexID": -1,
"contact": "",
"dataHandle": 1584981175839,
"description": "",
"driveBays": 0,
"drives": [],
"embeddedHypervisorPresence": false,
"encapsulation": {
   "encapsulationMode": "notSupported"
},
"errorFields": [
   { "HostAndDomain": "NO_CONNECTOR" },
   { "PhysicalAndLocation": "NO_CONNECTOR" },
   { "Encapsulation": "NO_CONNECTOR" },
   { "Memory": "NO_CONNECTOR" },
   { "ServerFirmwareData": "NO_CONNECTOR" },
   { "RackCPU": "NO_CONNECTOR" },
   { "ServerOnboardPciDevices": "NO_CONNECTOR" },
   { "BootMode": "NO_CONNECTOR" },
   { "SecureBootMode": "NO_CONNECTOR" },
   { "BootOrder": "NO_CONNECTOR" },
   { "FlashDimm": "NO_CONNECTOR" },
   { "HostMacAddress": "NO_CONNECTOR" },
   { "VnicMode": "NO_CONNECTOR" },
   { "RemotePresenceEnabled": "NO_CONNECTOR" },
   { "ActivationKey": "NO_CONNECTOR" },
   { "LanOverUsbMode": "NO_CONNECTOR" },
   { "ServerStaticMetrics": "NO_CONNECTOR" },
   { "ScalableComplexPartitionUUIDData": "NO_CONNECTOR" },
   { "ActiveAlerts": "NO_CONNECTOR" },
   { "PFAConfiguration": "NO_CONNECTOR" },
   { "ServerIPaddresses": "NO_CONNECTOR"  },
   { "FaceplateInfo": "NO_CONNECTOR" },
   { "IOCompatibilityData": "NO_CONNECTOR" },
   { "LanOverUsbPortForwardingModes": "NO_CONNECTOR" },
   { "ServerConfigFiles": "NO_CONNECTOR" }
],
"excludedHealthState": "Normal",
"expansionCards": [],
"expansionCardSlots": 0,
"expansionProducts": [],
"expansionProductType": "",
"faceplateIDs": [],
"firmware": [],
"flashStorage": [],
"FRU": "",
"fruSerialNumber": "",
"hasOS": false,
```

```
"hostMacAddresses": "",
"ipInterfaces": [],
"isConnectionTrusted": "true",
"isITME": false
"isRemotePresenceEnabled": false,
"isScalable": false,
"lanOverUsb": "disabled",
"lanOverUsbPortForwardingModes": [],
"leds": [],
"location": {
   "location": "",
   "lowestRackUnit": 0,
   "rack": "",
   "room": ""
},
"logicalID": -1,
"m2Presence": false,
"machineType": "",
"manufacturer": "",
"manufacturerId": "",
"memoryModules": [],
"memorySlots": 0,
"mgmtProcType": "UNKNOWN",
"model": "",
"name": "Node 07",
"nist": {
   "currentValue": "Unknown",
   "possibleValues": ["Nist_800_131A_Strict","unsupported","Compatibility"]
},
"onboardPciDevices": [],
"osInfo": {
   "description": "",
   "storedCredential": ""
},
"overallHealthState": "Normal",
"parent": {
   "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
   "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
},
"partitionID": -1,
"partNumber": "",
"pciCapabilities": [],
"pciDevices": [],
"ports": [],
"posID": "",
"powerAllocation": {
   "maximumAllocatedPower": 0,
   "minimumAllocatedPower": 0
},
"powerStatus": 0,
"powerSupplies": [],
"primary": false,
"processors": [],
"processorSlots": 0,
"productId": "",
"productName": "",
"raidSettings": [],
"secureBootMode": {
   "currentValue": "",
   "possibleValues": []
},
```

```
    "securityDescriptor": {
       "managedAuthEnabled": false,
       "managedAuthSupported": true,
       "publicAccess": false,
       "roleGroups": ["lxc-supervisor"],
       "storedCredentials": {
          "description": "Credentials for null",
          "id": "1703",
          "userName": "USERID"
       },
       "uri": "nodes/dummy-671d5d9ebb4440a4-chassis(1)-blade(7)"
    },
    "serialNumber": "",
    "slots": [7],
    "status": {
       "message": "managed",
       "name": "MANAGED"
    },
    "subSlots": [],
    "subType": "",
    "tlsVersion": {
       "currentValue": "Unknown",
       "possibleValues": ["unsupported","TLS_12","TLS_11","TLS_10"]
    },
    "type": "ITE",
    "uri": "nodes/DUMMY-671D5D9EBB4440A4-CHASSIS(1)-BLADE(7)",
    "userDefinedName": "",
    "userDescription": "",
    "uuid": "DUMMY-671D5D9EBB4440A4-CHASSIS(1)-BLADE(7)",
    "vnicMode": "disabled",
    "vpdID": ""
}],
"overallHealthState": "Warning",
"parent": {
    "uri": "cabinet/",
    "uuid": ""
},
"partNumber": "88Y6660",
"passThroughModules": [],
"posID": "14",
"powerAllocation": {
    "allocatedOutputPower": 1504,
    "midPlaneCardMaximumAllocatedPower": 38,
    "midPlaneCardMinimumAllocatedPower": 38,
    "remainingOutputPower": 3506,
    "totalInputPower": 5445,
    "totalOutputPower": 5010
},
"powerSupplies": [{
    "dataHandle": 0,
    "cmmDisplayName": "Power Supply 06",
    "cmmHealthState": "Non-Critical",
    "description": "Power Supply",
    "excludedHealthState": "Warning",
    "firmware": [{
       "build": "",
       "classifications": [],
       "date": "",
       "name": "Power Supply Firmware",
       "revision": "0",
       "role": "",
```

```
            "softwareID": "",
            "status": "",
            "type": "Power Supply Firmware",
            "version": ""
         }                              ],
         "FRU": "69Y5817",
         "fruSerialNumber": "ZK125115V0VS",
         "hardwareRevision": "5.0",
         "healthState": "NA",
         "inputVoltageIsAC": true,
         "inputVoltageMax": -1,
         "inputVoltageMin": -1,
         "leds": [{
            "color": "Green",
            "location": "Planar",
            "name": "OUT",
            "state": "Off"
         }],
         "machineType": "",
         "manufactureDate": "2211",
         "manufacturer": "IBM",
         "manufacturerId": "20301",
         "model": "",
         "name": "Power Supply 06",
         "overallHealthState": "Warning",
         "parent": {
            "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
            "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
         },
         "partNumber": "69Y5801",
         "posID": "60",
         "powerAllocation": {
            "totalInputPower": 0,
            "totalOutputPower": 343
         },
         "powerState": "Unknown",
         "productId": "303",
         "productName": "IBM 2500 W Power Supply",
         "serialNumber": "",
         "slots": [6],
         "type": "PowerSupply",
         "uri": "powerSupply/04382F96885411E00095009500950095",
         "userDescription": "",
         "uuid": "04382F96885411E00095009500950095",
         "vpdID": "128"
      }],
      "powerSupplySlots": 6,
      "productId": "336",
      "productName": "IBM Chassis Midplane",
      "securityDescriptor": {
         "managedAuthEnabled": false,
         "managedAuthSupported": true,
         "publicAccess": false,
         "roleGroups": ["lxc-supervisor"],
         "storedCredentials": {
            "description": "Credentials for null",
            "id": "1703",
            "userName": "USERID"
         },
         "uri": "chassis/671d5d9ebb4440a49d9daf08a9edfb36"
      },
```

```
"SecurityPolicy": {
   "cmmPolicyState": "ACTIVE",
   "cmmPolicyLevel": "SECURE"
},
"serialNumber": "23DVG73",
"status": {
   "message": "MANAGED",
   "name": "MANAGED"
},
"switches": [{
   "accessState": "Online",
   "accessStateRecords": [{
      "health": "OFFLINE",
      "ipAddress": "10.241.53.20",
      "messageBundle": "com.lenovo.lxca.inventory.base.bundle.connections.messages",
      "messageDisplay": "Authentication failed occurred due to HTTP 401 - Unauthorized (OpenPegasus Error: \
      "messageID": "0510",
      "messageParameter": "HTTP 401 - Unauthorized (OpenPegasus Error: \"User Unauthorized\")",
      "protocol": "CIM",
      "username": "USERID",
      "timestamp": 1584709239559,
      "trusted": true
   }],
   "attachedNodes": [],
   "backedBy": "real",
   "cmmDisplayName": "IO Module 04",
   "cmmHealthState": "Normal",
   "dataHandle": 1584981209777,
   "description": "FC5022 16Gb SAN Scalable Switch",
   "deviceName": "FC5022",
   "errorFields": [{
      "IOCompatibilityData": "FETCH_FAILED"
   }],
   "excludedHealthState": "Normal",
   "firmware": [{
      "classifications": [],
      "build": "",
      "date": "2016-04-19T04:00:00Z",
      "name": "Main Application",
      "status": "Active",
      "type": "Main Application",
      "version": "7.4.1c"
   }],
   "FRU": "00Y3329",
   "fruSerialNumber": "Y050UZ67D009",
   "ipInterfaces": [{
      "IPv4DHCPmode": "DHCP_THEN_STATIC",
      "IPv4enabled": true,
      "IPv6enabled": true,
      "IPv6DHCPenabled": true,
      "IPv6statelessEnabled": true,
      "IPv6staticEnabled": false,
      "label": "",
      "name": "ioe0"
   }],
   "leds": [{
      "color": "Amber",
      "location": "FrontPanel",
      "name": "FRU Fault",
      "state": "Off"
   }],
```

```
            "machineType": "",
            "manufacturer": "LNV",
            "manufacturerId": "20301",
            "model": "",
            "name": "IO Module 04",
            "ntpPushEnabled": false,
            "ntpPushFrequency": 17,
            "overallHealthState": "Normal",
            "parent": {
               "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
               "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36"
            },
            "partNumber": "00MM452",
            "ports": [],
            "posID": "17",
            "powerAllocation": {
               "maximumAllocatedPower": -1,
               "minimumAllocatedPower": -1
            },
            "powerState": "On",
            "productId": "329",
            "productName": "Flex System FC5022 24-port 16Gb SAN Scalable Switch",
            "protectedMode": "Not supported",
            "securityDescriptor": {
               "managedAuthEnabled": false,
               "managedAuthSupported": true,
               "publicAccess": false,
               "roleGroups": [],
               "storedCredentials": {
                  "description": "Credentials for null",
                  "id": "1702",
                  "userName": "USERID"
               },
               "uri": "switches/AE986BEC1DD1B201684FC4F57C3B16B6"
            },
            "serialNumber": "",
            "slots": [4],
            "stackMode": "N/A",
            "type": "Switch",
            "uri": "switches/AE986BEC1DD1B201684FC4F57C3B16B6",
            "userDefinedName": "",
            "userDescription": "",
            "uuid": "AE986BEC1DD1B201684FC4F57C3B16B6",
            "vpdID": "309"
         }],
         "switchSlots": 4,
         "tlsVersion": {
            "currentValue": "TLS_12_Server",
            "possibleValues": ["TLS_12_Server","unsupported","TLS_12_Server_Client","SSL_30"]
         },
         "type": "Chassis",
         "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
         "userDefinedName": "SN#Y010BG57Y01G",
         "userDescription": "",
         "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
         "vpdID": "336"
      }
   }],
   "complexList": [],
   "height": 52,
   "nodeList": [],
```

```
            "location": "",
            "placeholderList": [],
            "room": "",
            "storageList": [],
            "switchList": [],
            "UUID": "STANDALONE_OBJECT_UUID"
        }]
    }
}
```

Capítulo 4. Gerenciando espaço em disco

É possível gerenciar a quantidade de espaço em disco usada pelo Lenovo XClarity Administrator movendo arquivos de dados grandes que não são necessários imediatamente para um compartilhamento remoto ou excluindo recursos que não são mais necessários.

Sobre esta tarefa

Para determinar quanto espaço em disco está sendo utilizado atualmente, clique em **Painel** na barra de menu do XClarity Administrator. O uso de espaço em disco no repositório e compartilhamentos remotos está listado na seção XClarity Administrator Atividade.

Procedimento

Conclua uma ou mais das etapas a seguir para liberar espaço em disco movendo arquivos para um compartilhamento remoto e excluindo recursos desnecessários.

- **Excluir recursos desnecessários**

  É possível excluir rapidamente arquivos do repositório local que não são mais necessários concluindo as etapas a seguir.

  1. Na barra de menu do XClarity Administrator, clique em **Administração → Limpeza de disco** para exibir a página Limpeza de Disco.
  2. Selecione os arquivos que deseja excluir. O cabeçalho da seção identifica a quantidade de espaço que será liberada quando os arquivos forem excluídos.
     - **Arquivos relacionados do sistema operacional**

       É possível excluir imagens do SO, arquivos de opção de inicialização e arquivos de software.
     - **Atualizações de firmware**

       É possível excluir arquivos de carga útil para todos os drivers de dispositivo do SO associados aos UpdateXpress System Packs (UXSPs) e drivers de dispositivo individuais que estão no estado Baixado.

       É possível excluir arquivos de carga útil para atualizações de firmware individuais que estão no estado Baixado e não são usadas em uma política de conformidade de firmware.

       É possível excluir arquivos de carga útil para atualizações do servidor de gerenciamento que estão no estado Baixado.

       Nota: Quando o repositório das atualizações de firmware está localizado em um compartilhamento remoto, não é possível usar a função de limpeza de disco para excluir atualizações de firmware individuais e UXSPs.
     - **Arquivos de dados de serviço**

       Quando ocorre um evento de serviço em um dispositivo, os dados de serviço são coletados automaticamente para esse dispositivo. Os dados de serviço são capturados automaticamente para o servidor de gerenciamento sempre que ocorre uma exceção no XClarity Administrator. É recomendável excluir periodicamente esses arquivos se o XClarity Administrator e os dispositivos gerenciados estiver funcionando sem problemas.

       Quando as atualizações do servidor de gerenciamento são aplicadas com êxito, os arquivos de atualização são removidos automaticamente do repositório.

© Copyright Lenovo 2015, 2025

3. Clique em **Excluir Selecionado**.
4. Revise a lista de arquivos selecionados e clique em **Excluir**.

- **Limpeza sem uso dos pacotes de atualização de firmware**

  É possível excluir todos os pacotes de firmware não usadas no repositório de atualizações clicando em **Fornecimento → Atualizações de Firmware: Repositório** na barra de menus do XClarity Administrator e, em seguida, clicando em **Todas as Ações → Limpar repositório**.

  É possível escolher entre manter ou remover as versões mais recentes se elas não estão em uso.

  Um trabalho é criado para realizar esta solicitação. Você pode monitorar o andamento do trabalho clicando em **Monitoramento → Trabalhos** na barra de menus do XClarity Administrator.

- **Mova os pacotes de atualização de firmware para um repositório remoto**

  Por padrão, o Lenovo XClarity Administrator usa um repositório local (interno) para armazenar atualizações de firmware. É possível liberar o espaço em disco que está disponível para o repositório local do XClarity Administrator usando um compartilhamento remoto montado no SSH File System (SSHFS) como repositório remoto. É possível então usar arquivos de atualização de firmware diretamente do repositório remoto para manter a conformidade de firmware em seus dispositivos. Para obter mais informações, consulte Usando um repositório remoto para atualizações de firmware na documentação online do XClarity Administrator.

  Ao alterar o local do repositório de atualizações de firmware, é possível optar por copiar todas as atualizações de firmware do repositório original no novo repositório.

  Os arquivos de atualização de firmware no repositório original *não* são limpos automaticamente depois de alternar locais.

  Dica: O repositório de atualizações remotas pode ser compartilhado por vários servidores de gerenciamento do XClarity Administrator.

  Para mover atualizações de firmware para um repositório de atualizações de firmware remotas, conclua as etapas a seguir.

  1. Adicione um compartilhamento remoto XClarity Administrator (consulte Gerenciando compartilhamentos remotos na documentação on-line do XClarity Administrator).
  2. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Atualizações de Firmware: Repositório**. A página Repositório das Atualizações de Firmware é exibida.
  3. Clique em **Todas as Ações → Alternar local do repositório** para exibir a caixa de diálogo Alternar Local do Repositório.
  4. Selecione o compartilhamento remoto que você acabou de criar na lista suspensa **Local do repositório**.
  5. Selecione **Copiar pacotes de atualização do repositório atual no novo repositório** para copiar arquivos de atualização de firmware para o novo local do repositório antes de alternar o local do repositório.
  6. Clique em **OK**.

     Um trabalho é criado para copiar pacotes de atualização de firmware para o novo repositório. Você pode monitorar o andamento do trabalho clicando em **Monitoramento → Trabalhos** na barra de menus do XClarity Administrator.
  7. Limpe os arquivos de atualização de firmware no repositório local.
     a. Alterne o local para o repositório local clicando em **Todas as Ações → Alternar local do repositório**, selecione o **Repositório Local** para o local do repositório e, em seguida, clique em **OK**.

b. Clique na guia **Atualizações Individuais**, clique na caixa de seleção select-all na tabela para selecionar todas as atualizações de firmware e, em seguida, clique no ícone **Excluir pacotes de atualização completas** ( )

c. Clique na guia **UpdateXpress System Pack (UXSP)**, clique na caixa de seleção select-all na tabela para selecionar todos os UXSPs e, em seguida, clique no ícone **Excluir UXSP e política associada** ( )

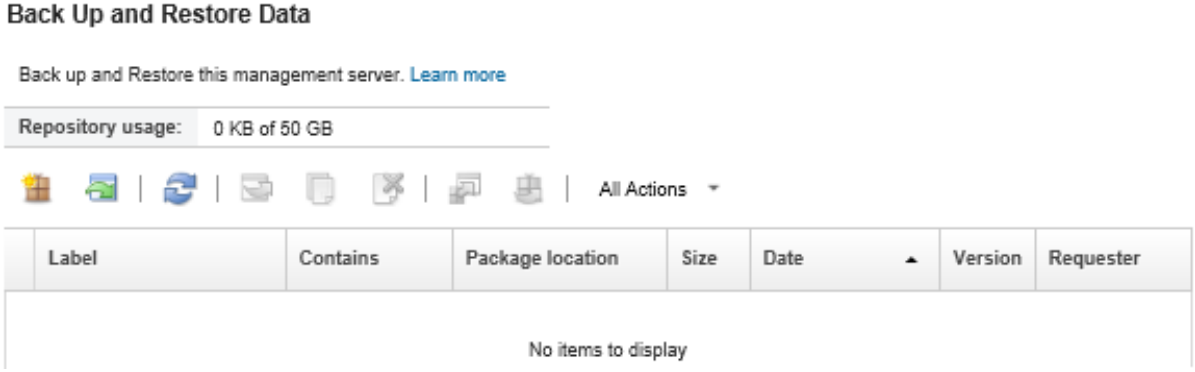
d. Alterne o local de volta para o repositório remoto clicando em **Todas as Ações → Alternar local do repositório**, selecione o novo repositório remoto para o local do repositório e, em seguida, clique em **OK**.

- **Mover XClarity Administrator backups para um compartilhamento remoto**

  É possível liberar espaço em disco que está disponível para o repositório local do XClarity Administrator movendo backups do XClarity Administrator para um compartilhamento remoto. No entanto, não é possível usar os arquivos diretamente no compartilhamento remoto. Para usar os arquivos, você deverá movê-los de volta para o repositório local XClarity Administrator. Para obter mais informações sobre compartilhamentos remotos, consulte Gerenciando compartilhamentos remotos na documentação online do XClarity Administrator.

  Importante: É recomendável fazer download de backups para seu sistema local ou copiar os backups em um compartilhamento remoto antes de excluir os backups em XClarity Administrator.

  1. Na barra de menu XClarity Administrator, clique em **Administration → Back Up and Restore Data** para exibir a página Back Up and Restore Data.

     A coluna **Local do pacote** identifica se o backup está armazenado localmente no repositório local do XClarity Administrator ou em um compartilhamento remoto.

  2. Selecione o backup e clique no ícone **Copiar backup** ( ) para exibir a caixa de diálogo Copiar backup.
  3. Escolha o compartilhamento remotopara armazenar o backup.
  4. Clique em **Copiar**.
  5. Monitore o andamento da cópia na página Trabalhos. Quando a cópia for concluída, selecione o backup novamente e clique no ícone **Excluir backup** ( ) para exibir a caixa de diálogo Excluir backup.
  6. Selecione "Local" para o local.
  7. Clique em **Excluir**.

Capítulo 5. Problemas de descoberta e gerenciamento

Use estas informações para solucionar problemas de descoberta de dispositivo e gerenciamento.

Não é possível descobrir um dispositivo

Use estas informações para solucionar problemas ao localizar dispositivos gerenciáveis.

1. Verifique se o Lenovo XClarity Administrator é compatível com o dispositivo. Para obter uma lista de dispositivos compatíveis, consulte Página da Web Suporte do XClarity Administrator – Compatibilidade, clique na guia **Compatibilidade** e, em seguida, clique no link para os tipos de dispositivo apropriados.
2. Verifique se o dispositivo está acessível na rede em XClarity Administrator e se XClarity Administrator está acessível na rede do dispositivo.
3. Verifique se as portas corretas estão abertas no firewall. Para obter informações sobre requisitos de porta, consulte Disponibilidade de porta na documentação online do XClarity Administrator.
4. Verifique se SLP unicast e multicast está ativado na rede.
5. Para servidores ThinkServer:
   a. Usando a interface da Web de gerenciamento do servidor, verifique se o nome do host do servidor está configurado com um nome do host ou endereço IP válido.
   b. Verifique se SLP está ativado e se o nome do host está ativado no ThinkServer System Manager (TSM).
      - Para determinar quais servidores ThinkServer têm SLP ativado, envie uma solicitação SLP para consultar o serviço WBEM usando sua ferramenta SLP preferencial.
        ```
        $ slptool findsrvs service:wbem
        service:wbem:http://<TSM_IP>:5988,65535
        service:wbem:https://<TSM_IP>:5989,65535
        ```
      - Para determinar se SLP está ativado em um ThinkServer específico, envie uma solicitação SLP para consultar o serviço WBEM usando sua ferramenta SLP preferencial.
        ```
        $ slptool unicastfindattrs <TSM_IP> service:wbem
        (template-type=wbem),(template-version=2.0),(template-url-syntax=service:URL),
        (service-hi-name=qom),(service-hi-description=Quasi Object Manager 1.0.0),
        (CommunicationMechanism=cim-xml),(CommunicationMechanismsVersion=1.0),
        (MultipleOperationsSupported=false),(AuthenticationMechanismsSupported=Basic),
        (InteropSchemaNamespace=root/interop),(service-id=Lenovo G5 WBEM Service)
        ```
      - Se um dispositivo não responder à solicitação SLP, reinicie o firmware de TSM enviando um comando IPMI ao TSM usando os seguintes parâmetros. Pode levar vários minutos para o TSM reiniciar.
        ```
        NetFn = 0x06
        Command = 0x03
        Data = ()
        ```
        O seguinte exemplo ativa SLP usando a ferramenta de código-fonte `ipmitool`.
        ```
        $ ipmitool -H <TSM_IP> -U <ipmi_user> -P <ipmipassword> raw 0x06 0x03
        ```
6. Para comutadores RackSwitch, verifique se SLP está ativado e se o nome do host está definido na configuração do comutador.
   - Os comutadores ThinkSystem série DB não podem ser descobertos. Para gerenciar esses comutadores, insira manualmente o endereço IP do comutador clicando em **Entrada Manual** na página Descobrir e Gerenciar Novos Dispositivos.

© Copyright Lenovo 2015, 2025

- Os comutadores NVIDIA Mellanox não podem ser descobertos. Para gerenciar esses comutadores, insira manualmente o endereço IP do comutador clicando em **Entrada Manual** na página Descobrir e Gerenciar Novos Dispositivos.
- Para outros comutadores, verifique se SLP está ativado e se o nome do host está definido na configuração do comutador.
  - Para determinar quais comutadores têm SLP ativado, envie a seguinte solicitação SLP multicast usando sua ferramenta SLP preferencial.

    Nota: Essa solicitação localiza somente os comutadores que estão na mesma sub-rede da ferramenta SLP em execução.

    ```
    $ slptool findsrvs service:io-device.Lenovo:management-module
    service:io-device.Lenovo:management-module://<RackSwitch IP>,64225
    ```
  - Para determinar se SLP está ativado em um comutador específico, envie a seguinte solicitação SLP unicast usando sua ferramenta SLP preferencial.
    ```
    $ slptool findattrs service:io-device.Lenovo:management-module://<RackSwitch IP>
    (level=1.0),(Type=switch),(data-protocols=ethernet),(serial-number=US7116000D),
    (sysoid=1.3.6.1.4.1.26543.1.7.6),(ipv4-enabled=TRUE),(ipv4-address=<RackSwitch IP>),
    (ipv6-enabled=FALSE),ipv6-addresses,(ipv4-mgmt-protocols=http:80:true,https:443:true,
    telnet:23:true,ssh:22:true,snmpv1v2v3:161:true,snmpv3only:161:false),
    (snmp-engineid=80:00:67:af:03:08:17:f4:33:d3),
    (ssh-fingerprint=8a:43:cb:be:47:d9:31:37:7a:3b:80:f6:dd:00:61:a6),
    (deviceName=<RackSwitch hostname>)
    ```

7. Para dispositivos Lenovo Storage (que não sejam os ThinkSystem Série DE), verifique se SLP está ativado e se sua rede não está bloqueando a comunicação SLP entre o XClarity Administrator e o dispositivo de armazenamento.
   - Para determinar quais dispositivos de armazenamento têm SLP ativado, envie uma solicitação SLP para consultar o serviço API usando sua ferramenta SLP preferencial.
     ```
     $ slptool findsrvs service:api
     service:api:https://<CONTROLLER_IP>:443/api,65535
     service:api:https://<CONTROLLER_IP>:443/api,65535
     ```
   - Para determinar se SLP está ativado em um dispositivo de armazenamento específico, envie uma solicitação SLP para consultar o serviço API usando sua ferramenta SLP preferencial.
     ```
     $ slptool unicastfindattrs <CONTROLLER_IP> service:api
     (x-system-name=S3200_5.65),(x-system-location=rack\2Crack\2Crack),(x-system-contact=Support contact),
     (x-system-information=S3200_65),(x-vendor-name=Lenovo),(x-product-id=S3200),(x-product-brand=Storage),
     (x-midplane-serial-number=00C0FF2682A8),(x-platform-type=Gallium),(x-bundle-version=""),
     (x-build-date=""),(x-health=OK),(x-wwnn=208000c0ff2682a8),(x-mac-address=00:00:00:00:00:EB)
     ```

   Se um dispositivo de armazenamento não responder à solicitação SLP:

   - Verifique se a rede permite comunicação SLP entre os dispositivos.
   - Verifique se os dispositivos de armazenamento têm **Storage Management Initiative Specification (SMI-S)** ativado, e reinicie o dispositivo de armazenamento usando a interface da Web de gerenciamento ou a CLI.

Não é possível gerenciar um dispositivo

Use estas informações para solucionar problemas ao gerenciar dispositivos.

1. Verifique se o dispositivo é compatível com Lenovo XClarity Administrator. Para obter informações sobre suporte ao dispositivo, consulte Página da Web Suporte do XClarity Administrator – Compatibilidade, clique na guia **Compatibilidade** e, em seguida, clique no link para os tipos de dispositivo apropriados.
2. Verifique se o dispositivo está acessível na rede em XClarity Administrator e se XClarity Administrator está acessível na rede do dispositivo.

3. Verifique se todas as portas apropriadas para o gerenciamento de evento estão abertas na rede e no firewall. Para obter informações sobre requisitos de porta, consulte Disponibilidade de porta na documentação online do XClarity Administrator.
4. Verifique se o firmware mínimo necessário está instalado em cada servidor que você deseja gerenciar usando o XClarity Administrator. É possível localizar os níveis mínimos de firmware necessários em Página da Web Suporte do XClarity Administrator – Compatibilidade clicando na guia **Compatibilidade** e, em seguida, clicando no link para os tipos de dispositivo apropriados.
5. Verifique se não há problemas com o certificado do servidor XClarity Administrator.
   a. Verifique se o certificado do servidor XClarity Administrator não expirou.
   b. Verifique se o certificado do servidor XClarity Administrator tem um endereço IP válido no SubjectAltName (consulte Implantando certificados de servidor personalizado no XClarity Administrator na documentação online do XClarity Administrator).
6. Verifique se a data no servidor não entra em conflito com o certificado LDAP. Por exemplo, se o certificado LDAP for válido de **2022/8/3** a **2024/11/3**, mas a data do XCC for **2000-04-15**, o servidor não passará na verificação do TLS.
7. Verifique se CIM sobre HTTPS está ativado no dispositivo.
   a. Faça login na interface da Web de gerenciamento do servidor usando a conta do usuário de `RECOVERY_ID`
   b. Clique em **Gerenciamento do IMM → Segurança**.
   c. Clique na guia **CIM sobre HTTPS** e certifique-se de que **Habilitar CIM sobre HTTPS** esteja selecionado.
8. Para servidores ThinkSystem SR635 e SR655:
   - Certifique-se de que um sistema operacional esteja instalado e que o servidor tenha sido inicializado para o SO, mídia inicializável montada ou efishell pelo menos uma vez para que o XClarity Administrator possa coletar o inventário desses servidores.
   - Verifique se a IPMI sobre LAN está ativada. O IPMI sobre LAN é desabilitado por padrão nesses servidores e deve ser habilitado manualmente para que os servidores possam ser gerenciados. Para ativar o IPMI sobre LAN usando o TSM, clique em **Configurações → Configuração de IPMI**. Talvez seja necessário reiniciar o servidor para ativar a mudança.
9. Se o certificado do servidor do dispositivo for assinado por uma autoridade de certificado externa, garanta que o certificado de autoridade de certificado e todos os certificados intermediários sejam importados para o armazenamento confiável do XClarity Administrator (consulte Implantando certificados de servidor personalizado em dispositivos gerenciados na documentação online do XClarity Administrator.
10. Verifique se as credenciais estão corretas para o dispositivo.

    Nota: Verifique se a senha segue as políticas de segurança e senha para o dispositivo. As políticas de segurança e senha podem variar.

    Quando o dispositivo é gerenciado por XClarity Administrator, o controlador de gerenciamento é colocado em gerenciamento de usuários centralizado. Isso significa que as contas de usuário definidas no servidor de autenticação interno ou externo do XClarity Administrator também são usadas para fazer login no controlador de gerenciamento. Uma nova conta de usuário local chamada RECOVERY_ID é criada, enquanto todas as contas locais são desativadas no controlador de gerenciamento.

    Se o processo de gerenciamento falhar ao configurar o gerenciamento de usuários centralizado, as contas de usuário locais no controlador de gerenciamento poderão ser desabilitadas. Execute as seguintes etapas para recuperar as contas de usuário locais:

    - Servidores Converged, NeXtScale e System x
      a. Faça login na interface da Web de gerenciamento do servidor usando a conta do usuário RECOVERY_ID.

b. Clique em **Gerenciamento do IMM → Usuário**.

c. Configure o método de autenticação do usuário no controlador de gerenciamento como **Local primeiro, depois LDAP**.

1) Clique em **Configurações de Login Global**. A caixa de diálogo Configurações de Login Global é exibida.

2) Clique na guia **Geral**.

3) Selecione **Local primeiro, depois LDAP** para o método de autenticação do usuário e clique em **OK**.

d. Exclua e recrie todas as contas de usuário locais (diferentes da conta do usuário RECOVERY_ID).

e. Tente gerenciar o chassi novamente usando a opção **Forçar gerenciamento** para apagar todas as assinaturas de CIM restantes da tentativa de gerenciamento anterior.

- Chassi

a. Faça login na CLI de gerenciamento do chassi em uma sessão SSH usando a conta do usuário RECOVERY_ID.

b. Execute o seguinte comando para desativar o gerenciamento de usuários centralizado e permitir que você faça a autenticação no controlador de gerenciamento e em outros componentes do chassi usando contas de usuário locais.

Nota: Após executar esse comando, a conta do usuário RECOVERY_ID é removida do registro do usuário, e a sessão de CLI é encerrada. Agora é possível autenticar-se no controlador de gerenciamento e em outros componentes do chassi usando contas de usuário locais.

```
fsmcm -off -T mm[p]
```

c. Tente gerenciar o chassi novamente usando a opção **Forçar gerenciamento** para apagar todas as assinaturas de CIM restantes da tentativa de gerenciamento anterior.

11. Para comutadores RackSwitch

- Verifique se SSH está ativado no comutador.
- Se definido, verifique se a senha "enable" usada para entrar no Modo Privilegiado/Exec do comutador está correto.

12. Para um servidor System x3950 X6, os servidores devem ser gerenciados como dois gabinetes 4U, cada com seu próprio Baseboard Management Controller.

13. Se a placa-mãe foi substituída no dispositivo, o dispositivo recebeu um novo número de série e UUID. Se desejar que o XClarity Administrator reconheça o dispositivo como o mesmo dispositivo antes da substituição, você deve atualizar o número de série e o UUID para corresponder ao que eram anteriormente. Consulte a documentação do dispositivo para obter instruções.

14. Se o dispositivo era gerenciado por XClarity Administrator, mas o gerenciamento não foi cancelado corretamente, consulte as informações a seguir para ver as etapas de recuperação:
    - Recuperando o gerenciamento de chassi com um CMM após uma falha no servidor de gerenciamento na documentação online do XClarity Administrator
    - Recuperando o gerenciamento do servidor após uma falha no servidor de gerenciamento na documentação online do XClarity Administrator
    - Recuperando um comutador RackSwitch cujo gerenciamento não foi cancelado corretamente na documentação online do XClarity Administrator
    - Recuperando o gerenciamento com um dispositivo de armazenamento Lenovo após uma falha no servidor de gerenciamento na documentação online do XClarity Administrator

Não é possível gerenciar um dispositivo de armazenamento devido a um certificado SSL/TSL inválido

Use estas informações para solucionar problemas ao gerenciar matrizes de armazenamento.

Cada dispositivo tem um certificado SSL autoassinado que o Lenovo XClarity Administrator usa para se comunicar com o dispositivo via HTTPS. Esse certificado tem um nome comum (CN) que identifica o nome do host (ou endereço IP) associado ao certificado. O nome comum representa o nome que é protegido pelo certificado SSL e o certificado é válido apenas se o nome do host da solicitação corresponde ao nome comum do certificado. Portanto, se o endereço IP da matriz de armazenamento for alterado, o certificado existente se tornará inválido e o XClarity Administrator não poderá gerenciá-lo devido a um certificado SSL/TSL inválido.

Para resolver esse problema:

- Certifique-se de que o endereço IP no valor CN do certificado enviado de dispositivos de armazenamento DE esteja no formato IPv4.
- Certifique-se de que o certificado SSL/TSL existente seja válido
  - Para matrizes de armazenamento Lenovo ThinkSystem DE, redefina o certificado de gerenciamento na matriz de armazenamento como o certificado autoassinado de fábrica. Para obter mais informações, consulte Redefinir certificados de gerenciamento na documentação online do ThinkSystem Storage Série DE
  - Para matrizes de armazenamento Lenovo ThinkSystem DS, reinicie os controladores de gerenciamento no dispositivo de armazenamento usando a interface da web de gerenciamento ou a CLI para gerar novamente o certificado com o CN correto usando o novo endereço IP ou o nome do host.

Não é possível gerenciar um comutador devido a um certificado SSL/TSL inválido

Use essas informações para solucionar problemas de certificado ao gerenciar comutadores que executam o CNOS.

Cada dispositivo tem um certificado SSL autoassinado que o Lenovo XClarity Administrator usa para se comunicar com o dispositivo via HTTPS. Se você excluir ou regenerar o certificado no comutador, a comunicação entre o comutador e o XClarity Administrator falhará, e o comutador aparecerá offline.

Para corrigir esse problema, na página Todos os comutadores, selecione o comutador e clique em **Todas as Ações → Segurança → Resolver Certificados Não Confiáveis**.

Não é possível recuperar a conectividade de um chassi do Flex System gerenciado após a substituição da placa de LED traseira ou do conjunto do painel intermediário

O Lenovo XClarity Administrator gerencia dispositivos usando o identificador universal exclusivo (UUID) e certificados confiáveis com base em UUID. Para o chassi do Flex System, o UUID é armazenado como parte dos dados vitais do produto (VPD) na placa de LED traseira que se encontra no conjunto do painel intermediário. Ao substituir a placa de LED traseira ou o conjunto do painel intermediário, você deve transferir o UUID das placas de LED traseiras para a nova placa de LED traseira.

1. Obtenha o UUID do chassi. Se o chassi não estiver operacional, é possível obter o UUID ao entrar em contato com o Suporte e fornecer o tipo de máquina e o número de série, que você pode encontrar em um dos rótulos do chassi.
2. Altere o UUID de um chassi. Consulte o Documentação online do Lenovo Flex System do dispositivo para obter instruções de alteração do painel intermediário/placa de LED traseira e UUID.
3. Resolva certificados não confiáveis do chassi.
   a. Na barra de menu do XClarity Administrator, clique em **Hardware → Chassi**. A página Todos os Chassis é exibida.
   b. Selecione o chassi com a parte substituída.
   c. Clique em **Todas as Ações → Segurança → Resolver Certificados Não Confiáveis**.
   d. Clique em **Instalar Certificado**.

   O XClarity Administratorrecupera o certificado atual do chassi de destino e coloca-o no armazenamento confiável do XClarity Administrator, substituindo o certificado anterior desse chassi.
4. Atualize o inventário do chassi clicando em **Todas as Ações → Inventário → Atualizar Inventário**.

Não é possível recuperar a conectividade de um servidor gerenciado depois de substituir a placa-mãe

O Lenovo XClarity Administrator gerencia dispositivos usando o identificador universal exclusivo (UUID) e certificados confiáveis com base em UUID. Para servidores, o UUID é armazenado como parte dos dados vitais do produto (VPD) na placa-mãe. Ao substituir a placa-mãe, você deve transferir o UUID da placa-mãe substituída para a nova placa-mãe.

Importante: É uma boa prática cancelar o gerenciamento do servidor antes de substituir a placa-mãe. Você pode reativar o gerenciamento do servidor após a substituição da placa-mãe.

Para transferir o UUID da placa-mãe substituída para a nova placa-mãe, execute as etapas a seguir.

1. Obtenha o UUID do servidor. Se o servidor não estiver operacional, é possível obter o UUID ao entrar em contato com o Suporte e fornecer o tipo de máquina e o número de série, que você pode encontrar em um dos rótulos do servidor.
2. Altere o UUID de um servidor. Consulte o manual de hardware do dispositivo para obter instruções de substituição de componentes e alteração do UUID.
3. Resolva certificados não confiáveis do servidor.
   a. Na barra de menu do XClarity Administrator, clique em **Hardware → Servidor**. A página Todos os Chassis é exibida.
   b. Selecione o servidor com a parte substituída.
   c. Clique em **Todas as Ações → Segurança → Resolver Certificados Não Confiáveis**.
   d. Clique em **Instalar Certificado**.

   O XClarity Administratorrecupera o certificado atual do servidor de destino e coloca-o no armazenamento confiável do XClarity Administrator, substituindo o certificado anterior desse servidor.
4. Atualize o inventário do servidor clicando em **Todas as Ações → Inventário → Atualizar Inventário**.

O encapsulamento não foi desativado depois do cancelamento do gerenciamento de um servidor

Se o encapsulamento global estiver ativado, o modo de encapsulamento mudará para "encapsulamento leve" quando você gerenciar um servidor. Normalmente, quando o gerenciamento do servidor é cancelado, o modo de encapsulamento volta para a configuração "normal" (desativado).

Se o modo de encapsulamento não mudar para "normal", conclua a etapa a seguir para desativar o encapsulamento:

1. Reinicie o Baseboard Management Controller.
2. Conecte o servidor de destino de um sistema que esteja configurado para usar o endereço IP do dispositivo virtual do Lenovo XClarity Administrator com falha. Depois, desative o encapsulamento abrindo uma sessão SSH para dispositivo e executando o seguinte comando:
   ```
   encaps lite off
   ```

Nó de cálculo não é exibido na interface do usuário depois do gerenciamento

Se você trocar um ThinkSystem SD530 em um chassi sem primeiro cancelar o gerenciamento de servidor existente, o novo servidor poderá não ser exibido na interface do usuário.

Para resolver esse problema, cancele o gerenciamento do chassi usando a opção Forçar e gerencie todos os ThinkSystem SD530 em um chassi novamente.

O estado de energia do servidor está incorreto

Se um servidor sem um sistema operacional estiver ligado, o Lenovo XClarity Administrator poderá mostrar um estado de energia incorreto para o servidor.

Execute um dos seguintes procedimentos para resolver esse problema:

- Certifique-se de que os servidores bare-metal estejam desligados.
- Para o XClarity Administrator v1.2.2 ou posterior, inicie o servidor para configuração BIOS/UEFI (F1) (consulte Ligando e desligando um servidor na documentação online do XClarity Administrator).

Capítulo 6. Problemas de instalação, remoção, atualização e migração de dados

Use estas informações para solucionar problemas de instalação, remoção, atualização e migração de dados.

A saída de vídeo não é exibida ao instalar o XClarity Administrator em Red Hat KVM

Ao instalar o dispositivo virtual Lenovo XClarity Administrator usando a interface do usuário KVM Red Hat, a saída de vídeo pode não ser exibida por meio do console, resultando em uma tela preta do console quando a máquina virtual XClarity Administrator é ligada em vez de exibir a faixa de máquina virtual com XClarity Administrator as informações de IP.

Para ver a saída de vídeo pelo console, certifique-se de que o dispositivo de vídeo esteja definido como **Cirrus** abrindo a tela de detalhes do hardware virtual XClarity Administrator e clicando em **Vídeo** na navegação esquerda. Por padrão, a interface do usuário do RedHat KVM define o dispositivo de vídeo como QXL.

As alterações de adaptador não são reconhecidas

Após remover, substituir ou configurar adaptadores, o Lenovo XClarity Administrator não reconhece as alterações.

Reinicie o dispositivo para permitir que o Baseboard Management Controller (BMC) reconheça as alterações. Consulte Documentação online do System x para obter mais informações.

Durante a configuração inicial, não é possível abrir o assistente de configuração Inicial em um navegador da Web

Use estas informações para solucionar problemas ao fazer a configuração inicial do Lenovo XClarity Administrator.

1. Certifique-se de que o sistema host físico atenda aos requisitos mínimos do sistema (consulte Sistemas de host compatíveis na documentação online do XClarity Administrator).
2. Certifique-se de usar um sistema virtual com suporte que atenda aos requisitos mínimos do sistema (consulte Sistemas de host compatíveis na documentação online do XClarity Administrator).
3. Verifique se a versão do seu navegador da Web é compatível com XClarity Administrator. Para obter uma lista de navegadores da Web compatíveis, consulte Acessando a interface da Web do XClarity Administrator na documentação online do XClarity Administrator.
4. Por padrão, o DHCP é ativado para configurações de rede. Verifique se um endereço IP válido foi atribuído fazendo login na máquina virtual local e executando o comando `ifconfig`. Se estiver usando uma configuração estática, siga estas etapas para configurar corretamente a instalação. Para obter mais informações, consulte Instalando o XClarity Administrator em ambientes baseados em VMware ESXi na documentação online do XClarity Administrator.

Falha inesperada de implantação do Lenovo XClarity Administrator

Use estas informações para solucionar problemas ao fazer a configuração inicial do Lenovo XClarity Administrator.

© Copyright Lenovo 2015, 2025

1. Verifique no log de eventos se há eventos relacionados a implantação e resolva esses eventos primeiro. Para obter mais informações sobre o log de eventos, consulte Trabalhando com eventos na documentação online do XClarity Administrator.
2. Certifique-se de que o sistema host físico atenda aos requisitos mínimos do sistema.
3. Certifique-se de que o sistema ou sistema virtual atenda aos requisitos mínimos do sistema.
4. Certifique-se de usar um gerenciador de máquina virtual com suporte.

Para obter mais informações sobre requisitos, consulte Sistemas de host compatíveis na documentação online do XClarity Administrator.

Falha na atualização do Lenovo XClarity Administrator

Use estas informações para solucionar problemas com a atualização do Lenovo XClarity Administrator.

1. Certifique-se de ter instalado quaisquer atualizações de pré-requisito.
2. Certifique-se de ter as permissões de usuário para instalar atualizações.

Para obter mais informações sobre como atualizar o XClarity Administrator, consulte Atualizando o servidor de gerenciamento do XClarity Administrator na documentação online do XClarity Administrator.

Capítulo 7. Problemas de conectividade

Use estas informações para solucionar problemas de conectividade.

Não é possível acessar o Lenovo XClarity Administrator

Use estas informações para solucionar problemas ao se conectar ao Lenovo XClarity Administrator.

Se o sistema operacional do host foi desligado inesperadamente, restaure o XClarity Administrator do backup mais recente. Para obter informações sobre backup e restauração do XClarity Administrator, consulte Fazendo backup e restaurando o XClarity Administrator na documentação online do XClarity Administrator.

Não é possível estabelecer uma conexão com o Lenovo XClarity Administrator usando o navegador Safari

Use estas informações para solucionar problemas ao se conectar ao XClarity Administrator usando o navegador da Web Safari.

Ao tentar se conectar à interface da Web do XClarity Administrator usando um navegador da Web Safari, é apresentada uma lista de certificados de cliente associados à sua conta de usuário. Escolher um desses certificados pode resultar em um erro "não é possível conectar-se". Esse problema pode ocorrer porque o navegador da Web Safari está tentando enviar um certificado de cliente ao XClarity Administrator, mas esse certificado de cliente não é válido para o servidor do XClarity Administrator. Para resolver o problema, exclua o certificado de cliente e tente se conectar novamente à interface da Web do XClarity Administrator. Para obter mais informações sobre esse problema ao usar um navegador Safari, consulte Página Problema com certificado de cliente Safari.

Não é possível efetuar login

Use estas informações para resolver problemas ao fazer login no Lenovo XClarity Administrator, no CMM e no Baseboard Management Controller.

Não é possível fazer login no Lenovo XClarity Administrator

Use estas informações para solucionar problemas ao fazer login no Lenovo XClarity Administrator.

1. Certifique-se de que a senha esteja correta e que as teclas Caps Lock e Number Lock não estejam ativas.
2. Verifique se a conta de usuário não está bloqueada. Se estiver bloqueada, um supervisor deverá desbloquear a conta de usuário (consulte Desbloqueando um usuário na documentação online do XClarity Administrator).
3. Verifique se a conta de usuário não está desativada. Se estiver desabilitada, um supervisor deverá habilitar a conta de usuário (consulte Ativando ou desativando um usuário na documentação online do XClarity Administrator).
4. Se você estiver usando um servidor de autenticação externo:
   a. Verifique se os grupos de função corretos estão configurados no XClarity Administrator. Para obter informações sobre grupos de função, consulte Criando um grupo de funções na documentação online do Lenovo XClarity Administrator.

© Copyright Lenovo 2015, 2025

b. Verifique se as contas de usuário estão definidas como membros de um desses grupos de função no servidor de autenticação externo.
c. Se você alterou a senha para a conta de cliente usada para associar XClarity Administrator ao servidor de autenticação externo, verifique se também atualizou a nova senha na interface da Web do XClarity Administrator:
    1) Faça login no XClarity Administrator usando o nome e senha do cliente definidos atualmente no XClarity Administrator (consulte Configurando um servidor de autenticação externo na documentação online do XClarity Administrator).
    2) Na barra de menu do XClarity Administrator, clique em **Administração → Segurança**.
    3) Clique no **Cliente LDAP** na seção Usuários e Grupos para exibir a caixa de diálogo Configurações do Cliente LDAP.
    4) Atualize a senha no campo **Senha do cliente** e clique em **Aplicar**.

    Se a conta do cliente for bloqueada devido a muitas tentativas login com falha após a senha ser alterada no servidor de autenticação externo, desbloqueie a conta diretamente no servidor de autenticação externa ou aguarde o período de bloqueio expirar antes de tentar alterar a senha no XClarity Administrator.
d. Se a senha da conta do cliente que é utilizada para associar o XClarity Administrator ao servidor de autenticação externo tiver expirado, execute as etapas a seguir para desbloquear a conta e alterar a senha do XClarity Administrator.
    1) Desbloqueie a conta do cliente e altere a senha do cliente no servidor de autenticação externo.
    2) Faça login no XClarity Administrator usando o nome e senha do cliente definidos atualmente no XClarity Administrator (consulte Configurando um servidor de autenticação externo na documentação online do XClarity Administrator).
    3) Na barra de menu do XClarity Administrator, clique em **Administração → Segurança**.
    4) Clique no **Cliente LDAP** na seção Usuários e Grupos para exibir a caixa de diálogo Configurações do Cliente LDAP.
    5) Atualize a senha no campo **Senha do cliente** e clique em **Aplicar**.
5. Se o sistema operacional do host foi desligado inesperadamente, e agora você está obtendo um erro de autenticação, restaure o XClarity Administrator do backup mais recente. Para obter informações sobre backup e restauração do XClarity Administrator, consulte Fazendo backup e restaurando o XClarity Administrator na documentação online do XClarity Administrator.

A senha de um usuário supervisor ou de recuperação local foi esquecida

Se não existir a conta do Isupervisor ou outra conta, será possível redefinir a senha para um usuário local com autoridade de **lxc-recovery** ou **lxc-supervisor** montando uma imagem ISO que contenha um arquivo de configuração com a nova senha.

Antes de iniciar

Atenção: Este procedimento não funciona para o XClarity Administrator v3.3.x e v3.4.x. Se você estiver usando uma dessas versões, entre em contato com o Suporte Lenovo para pedir assistência para recuperar o acesso ao XClarity Administrator.

Para redefinir a senha usando esse método, você deve ter acesso no sistema host XClarity Administrator.

O nome do usuário que está sendo redefinido deve ter autoridade **lxc-recovery** ou **lxc-supervisor**.

A senha deve aderir às mesmas regras de validação impostas pelo XClarity Administrator

Depois que a senha é redefinida, o usuário não é obrigado a alterá-la no primeiro acesso

Procedimento

Para criar e montar a imagem ISO, conclua as etapas a seguir.

1. Desligue a máquina virtual.
2. Crie um arquivo denominado `passwordreset.properties` que contenha os parâmetros a seguir.
   ```
   user=
   password=
   ```
   Você pode usar o comando echo para criar o arquivo, por exemplo:
   ```
   ECHO user=admin > ./ passwordreset.properties
   ECHO password=New_PasswOrd >> ./ passwordreset.properties
   ```
3. Crie uma imagem ISO que contenha o arquivo passwordreset.properties.

   Para criar uma imagem ISO no Windows, use seu software ISO favorito. No Linux, use o comando `mkisofs`, por exemplo

   ```
   mkisofs -V passreset -J -o ./passreset.iso ./passwordreset.properties
   ```

   em que **-V** é o rótulo do volume, **-J** corresponde ao formato Joliet, **-o** é o nome do arquivo de saída e **/passwordreset.properties** é o arquivo a ser incluído na imagem ISO
4. Faça upload da imagem ISO em um local adequado usando o Navegador de Armazenamento de Dados.
5. Monte a imagem ISO na máquina virtual.
   - **Para Citrix**:
     a. Monte a imagem .ISO de configuração como uma unidade de CD física para a máquina virtual.
     b. No Citrix, selecione a máquina virtual do XClarity Administrator.
     c. Clique na guia **Console**.
     d. Selecione o CD físico na lista de unidades.
   - **Para hosts Nutanix AHV:**
     a. Clique no menu **Configurações** (⚙) e, em seguida, clique em **Configuração de imagem** para exibir a caixa de diálogo Configuração de Imagem.
     b. Carregue a imagem `eth0_config.iso`.
        1) Na caixa de diálogo Configuração de imagem, clique em **Fazer Upload da imagem** para exibir a caixa de diálogo Criar imagem novamente.
        2) Especifique um nome para a imagem ISO.
        3) Selecione ISO para o tipo de imagem.
        4) Selecione **Carregar um arquivo**, clique em **Escolher arquivo** e selecione a imagem `eth0_config.iso`.
        5) Clique em **Salvar** para fazer upload do arquivo.
        6) Clique em **Fechar** para fechar a caixa de diálogo Configuração de Imagem.
     c. Aguarde até que os processos de upload sejam concluídos antes de continuar com as etapas de configuração. O círculo de status no menu indica quando os processos estão completos.
     d. Adicione um disco para a imagem `eth0_config.iso`.
        1) Na VM, clique em **Atualizar** na barra do menu inferior.
        2) Clique no ícone **Editar** para o disco CDROM para exibir a caixa de diálogo Editar Disco.
        3) Selecione **Clonar** do Serviço de Imagem para as operações.
        4) Selecione a imagem ISO que você criou anteriormente na lista de imagens.
        5) Clique em **Atualizar**.

6) Clique em **Salvar**.

- **Para hosts RedHat KVM:**
  a. No Virtual Machine Manager, selecione a máquina virtual e, em seguida, clique em **Adicionar Hardware** para exibir a caixa de diálogo Adicionar novo hardware Virtual.
  b. Clique na guia **Armazenamento**.
  c. Escolha **Selecionar armazenamento gerenciado ou outro existente**, clique em **Procurar** e selecione a imagem `eth0_config.iso`.
  d. Selecione **VirtIO** para o tipo de dispositivo.

  Nota: Para XClarity Administrator 1.4.0 e anterior, selecione **IDE** para o barramento de disco.
  e. Selecione **Nenhum** para o modo de cache.
  f. Clique em **Concluir**.
- **Para hosts VMware ESXi:**

  O arquivo ISO deve residir no armazenamento de dados do host ESXi para que possa ser montado como uma unidade de CD/DVD na máquina virtual XClarity Administrator.
  a. Clique com o botão direito na máquina virtual e clique em **Editar Configurações**.
  b. Clique em **Adicionar** para exibir o assistente Adicionar Hardware.
  c. Clique em **Unidade de CD/DVD** e em **Avançar**.
  d. Selecione **Usar imagem ISO** e clique em **Avançar**.
  e. Selecione a imagem ISO e clique em **Avançar**.
  f. Selecione o nó do dispositivo virtual e clique em **Avançar**.
  g. Clique em **Concluir**.
- **Para hosts Windows Hyper-V:**

  Importante: A máquina virtual deve ser desconectada antes de montar a imagem ISO.
  a. Na janela Gerenciador Hyper-V, clique com o botão direito no dispositivo virtual e clique em **Conectar** para exibir a janela Conexão de Máquina Virtual.
  b. Clique em **Mídia → Unidade de DVD → Inserir Disco**.
  c. Selecione a imagem ISO e clique em **Abrir**.

6. Ligue a máquina virtual e faça login na interface da Web do XClarity Administrator usando o nome de usuário e a senha que é especificada no arquivo `passwordreset.properties` (consulte Acessando a interface da Web do XClarity Administrator na documentação online do XClarity Administrator).
7. Desmonte a unidade e exclua a imagem ISO.
   - Para Citrix
     a. No hipervisor Citrix, selecione a máquina virtual do XClarity Administrator.
     b. Clique na guia **Console**.
     c. Limpe o CD físico associado com a ISO de configuração da lista de drivers.
   - **Para hosts Nutanix AHV:**
     a. Na VM, clique em **Atualizar** na barra do menu inferior.
     b. Clique no ícone **Editar** para o disco CDROM para exibir a caixa de diálogo Editar Disco.
     c. Clique no ícone **Ejetar**.
     d. Clique em **Salvar**.
   - **Para hosts VMware ESXi:**
     a. Clique com o botão direito na máquina virtual e clique em **Editar Configurações**.
     b. Selecione a unidade montada na lista de hardware e clique em **Remover**.

c. Clique em **OK**. A unidade agora está desconectada.
d. Clique com o botão direito na máquina virtual e clique em **Editar Configurações** novamente.
e. Selecione a unidade na lista de hardware e desmarque a caixa de seleção **Conectar ao ligar**.
f. Clique em **OK**.
g. Exclua a imagem ISO do armazenamento de dados.

- **Para hosts Windows Hyper-V:**
  a. Na janela Gerenciador Hyper-V, clique com o botão direito no dispositivo virtual e clique em **Conectar** para exibir a janela Conexão de Máquina Virtual.
  b. Clique em **Mídia → Unidade de DVD → Ejetar** *iso_image_name***.iso**.
  c. Exclua a imagem ISO do armazenamento de dados.

Não é possível fazer login no CMM gerenciado diretamente

Use estas informações para solucionar problemas ao fazer login diretamente em um CMM gerenciado.

1. Certifique-se de que a senha esteja correta e que as teclas Caps Lock e Number Lock não estejam ativas.
2. Verifique se as credenciais correspondam àquelas armazenadas no Lenovo XClarity Administrator. Se o CMM for gerenciado pelo XClarity Administrator, não será possível fazer login usando contas do CMM local. Para obter informações sobre o gerenciamento de usuários centralizado e descentralizado no XClarity Administrator, consulte Gerenciando o servidor de autenticação na documentação online do XClarity Administrator.

Não é possível fazer login diretamente no controlador de gerenciamento

Use estas informações para solucionar problemas ao fazer login diretamente em um controlador de gerenciamento.

1. Certifique-se de que a senha esteja correta e que as teclas Caps Lock e Number Lock não estejam ativas.
2. Verifique se as credenciais correspondam àquelas armazenadas no Lenovo XClarity Administrator.
3. Verifique se a versão do controlador de gerenciamento é compatível com XClarity Administrator.
4. Verifique se apenas um servidor XClarity Administrator está gerenciando o controlador de gerenciamento.

Não é possível acessar servidores gerenciados do Flex Power System

Use estas informações para resolver problemas ao fazer login diretamente em um servidor gerenciado do Flex Power System - Lenovo XClarity Administrator

Se você tiver um chassi que contenha servidores Flex System e Flex Power System, não conseguirá fazer login diretamente nos servidores Flex Power System devido a problemas de autenticação.

Quando o chassi é gerenciado por XClarity Administrator, o CMM é colocado em gerenciamento de usuários central. Isso significa que as contas de usuário definidas no servidor de autenticação interno ou externo também são usadas para fazer login no Chassis Management Module (CMM), e as contas de usuário do CMM local estão desativadas.

Para fazer login na interface da Web do controlador de gerenciamento de um servidor Flex Power System, use a conta RECOVERY_ID que foi criada quando o chassi era gerenciado pelo XClarity Administrator. Faça login no CMM usando essa conta e altere a senha. A senha deve ser alterada no primeiro acesso. Depois

que a senha for alterada, você poderá fazer login na interface da Web do controlador de gerenciamento do nó do Power System usando a conta RECOVERY_ID.

Se desejar gerenciar um nó do Flex Power System em um HMC (console de gerenciamento de hardware), conclua as seguintes etapas:

1. Faça login na interface da CLI de gerenciamento usando SSH.
2. Execute os seguintes comandos para configurar o método de autenticação do usuário no CMM para **Autenticação local e externa** e para excluir e recriar a conta USERID.
```
env -T mm[p]
accseccfg -am localldap
users -n USERID -clear
users -add -n USERID -p <password> -g Supervisor -ms 0
```

Perda repentina de conectividade com um dispositivo

Use estas informações para solucionar problemas ao conectar-se a um único dispositivo

1. Se o dispositivo que usa uma credencial armazenada estiver offline, verifique se as credenciais armazenadas não se tornaram expiradas ou inválidas. Se tiverem se tornado expiradas ou inválidas, conclua as etapas a seguir:
   a. Na página de todos os dispositivos, selecione o dispositivo a ser resolvido.
   b. Clique em **Todas as Ações → Segurança → Resolver Credenciais Armazenadas**.
   c. Altere a senha para a credencial armazenada ou selecione outra credencial armazenada a ser usada para o dispositivo gerenciado.
2. Verifique no log de eventos quaisquer eventos de rede do dispositivo e resolva-os primeiro. Para obter mais informações sobre o log de eventos, consulte Trabalhando com eventos na documentação online do Lenovo XClarity Administrator.
3. Verifique se o hardware de rede está funcionando corretamente para o caminho de conexão ao dispositivo.
4. Verifique se as portas corretas de comutador e firewall estão habilitadas para o dispositivo. Para obter informações sobre as portas necessárias, consulte Disponibilidade de porta na documentação online do XClarity Administrator.
5. Verifique se o dispositivo tem uma configuração de rede válida fazendo logon no dispositivo e verificando se o endereço IP é válido para a rede. Também é possível efetuar ping para testar se o dispositivo está visível na rede.
6. Tente fazer login diretamente no dispositivo.

Capítulo 8. Problemas de configuração do Lenovo XClarity Administrator

Use estas informações para solucionar problemas de configuração do Lenovo XClarity Administrator.

Problemas de configuração de LDAP externo

Use estas informações para solucionar problemas ao configurar um servidor de autenticação externo.

1. Verifique se o nome distinto raiz está correto.
2. Verifique se a conta de usuário do Lenovo XClarity Administrator é membro de pelo menos um grupo de funções. Para obter informações sobre grupos de função, consulte Criando um grupo de funções na documentação online do XClarity Administrator.
3. Verifique se o grupo de funções do XClarity Administrator coincide com pelo menos um grupo de funções no servidor LDAP.
4. Se você estiver usando endereços de servidor predefinidos, verifique se o endereço IP e o número da porta do servidor estão corretos.
5. Verifique se as configurações de DNS estão corretas.
6. Se estiver usando o DNS para descobrir servidores, verifique se o nome de domínio e o nome da floresta estão corretos.
7. Verifique se o nome distinto e senha do cliente estão corretos.

Para obter informações sobre a configuração do servidor de autenticação externo, consulte Configurando um servidor de autenticação externo na documentação online do XClarity Administrator.

O usuário não possui autorização suficiente para configurar servidores

Use estas informações para solucionar problemas ao configurar servidores gerenciados.

1. Verifique se você fez login em uma conta de usuário que pertence a um grupo de funções de supervisor ou administrativas. Para obter informações sobre funções de usuário, consulte Criando um grupo de funções na documentação online do Lenovo XClarity Administrator.
2. Entre em contato com o administrador do sistema para ter sua autoridade atualizada.

Problemas de ativação do Features on Demand

Use estas informações para solucionar problemas ao ativar recursos.

Siga as instruções da ferramenta que você está usando para aplicar a chave Features on Demand (FoD). Para obter mais informações sobre chaves FoD, consulte Visualizando chaves do Feature on Demand na documentação online do Lenovo XClarity Administrator.

VMware avisa que o driver VMXNET 3 não é suportado

Você poderá ver um aviso de que o driver de 3 VMXNET não é suportado quando instalar o Lenovo XClarity Administrator, editando as XClarity Administrator configurações do dispositivo virtual, realizando vmotion do XClarity Administrator, ou na infraestrutura de gerenciamento e monitoramento do VMware associado.

© Copyright Lenovo 2015, 2025

O XClarity Administrator dispositivo inclui o driver VMXNET 3. Você pode com segurança ignorar todos os erros do VMware dizem que não há suporte para o driver.

Capítulo 9. Problemas de desempenho

Use estas informações para solucionar problemas de desempenho.

Problemas de desempenho do Lenovo XClarity Administrator

Use estas informações para solucionar problemas de desempenho do Lenovo XClarity Administrator.

Se você tiver um ambiente com um grande número de dispositivos e de sessões de usuário simultâneas, e perceber um baixo desempenho do sistema, reduza o número de sessões de usuário simultâneas à interface da Web do XClarity Administrator ou aumente os recursos virtuais da CPU que estão alocados no dispositivo virtual.

Os recursos disponíveis para a máquina virtual (memória, tamanho do disco, processador) devem ser adequados para o número de dispositivos que estão sendo gerenciados. Para obter mais informações sobre requisitos de máquina virtual, consulte Sistemas de host compatíveis na documentação online do XClarity Administrator.

Para dicas e considerações sobre desempenho adicionais, consulte o XClarity Administrator: Guia de desempenho (White paper).

Desempenho de rede insatisfatório ou lento

Use estas informações para solucionar problemas de desempenho de rede insatisfatório ou lento.

1. Certifique-se de que nenhuma operação de rede relevante esteja sendo executada, como descobertas do sistema, implantações de sistema operacional ou atualizações de firmware contínuas.
2. Verifique se o restante da rede está funcionando em um uso nominal.
3. Se você tiver implementado a qualidade de serviço, certifique-se de que ela esteja configurada para permitir a conectividade ideal com o Lenovo XClarity Administrator.
4. Certifique-se de que sua topologia de rede esteja otimizada para conectividade com o XClarity Administrator e desempenho.

© Copyright Lenovo 2015, 2025

Capítulo 10. Problemas de segurança

Use estas informações para solucionar problemas de segurança, incluindo gerenciamento de usuários e autenticação.

Não é possível confiar no certificado SSL

A cadeia de certificados pode conter uma assinatura que é autoassinada ou não se origina de uma Autoridade de Certificação.

Portas 443, 3888, 9090, 50636, 50637

Cada instância do Lenovo XClarity Administrator tem uma Autoridade de Certificação (CA) exclusiva e gerada internamente. Por padrão, essas portas (usadas para comunicação entre o usuário e o dispositivo virtual ou entre os dispositivos gerenciados e o dispositivo virtual) usam um certificado assinado pela Autoridade de Certificação. Se não for possível confiar no certificado SSL, gere e implante um certificado de servidor assinado externamente personalizado no XClarity Administrator. Para obter mais informações, consulte Implantando certificados de servidor personalizado no XClarity Administrator na documentação online do XClarity Administrator.

Porta 8443

Cada instância do XClarity Administrator tem uma Autoridade de Certificação (CA) exclusiva que é usada somente para implantação do SO. Essa CA assina um certificado que é usado para o servidor de destino na porta 8443. Quando a implantação do SO é iniciada, o certificado da CA é incluído na imagem do SO que é enviada por push para o servidor de destino. Como parte do processo de implantação, esse servidor se conecta novamente à porta 8443 e verifica o certificado que essa porta fornece durante o handshake porque elas têm o certificado da CA.

Falha na validação de certificação do servidor

Use estas informações quando tentar instalar um certificado de servidor no Lenovo XClarity Administrator e a validação do certificado falhar.

Sobre esta tarefa

A validação de certificação do servidor poderá falhar quando o XClarity Administrator tentar:

- Conectar-se com dispositivos gerenciados usando CIM-XML sobre HTTPS.
- Acessar um servidor de autenticação externo usando LDAP seguro (se você tiver configurado uma conexão LDAP segura).
- Acessar um provedor de identidade SAML externo usando uma conexão segura (se você tiver configurado o SAML).
- Conectar-se aos servidores de arquivos remotos para importar imagens do SO (se você tiver configurado um servidor de imagem HTTPS).
- Conectar-se à Lenovo para obter informações de status de garantia.
- Conectar-se ao servidor de notificação por push da Apple e do Google (se as notificação por push do Lenovo XClarity Mobile estiverem habilitadas para um dispositivo iOS ou Android).

Procedimento

Para resolver esse problema, conclua as etapas a seguir.

© Copyright Lenovo 2015, 2025

- Verifique se o certificado ou o respectivo certificado de assinatura está no armazenamento confiável de Certificados Confiáveis ou de Certificados de Serviços Externos no XClarity Administrator. Para obter mais informações sobre certificados confiáveis e certificados de serviços externos, consulte Trabalhando com certificados de segurança na documentação online do XClarity Administrator.
- Verifique se o certificado não foi revogado (consulte Incluindo e substituindo uma lista de revogação de certificado na documentação online do XClarity Administrator).
- Verifique se o nome do host ou o endereço IP do servidor corresponde a um dos nomes alternativos de assunto ou ao nome comum (se a rede SAN não estiver presente) no certificado.
- Verifique se a data atual está entre as datas de "Início da validade" e "Fim da validade" no certificado.
- Verifique se o certificado está assinado com um algoritmo permitido: SHA1 ou mais forte se for o modo legado, ou SHA256 ou mais forte se for o modo estrito NIST (consulte Configurando o modo de criptografia e protocolos de comunicação na documentação online do XClarity Administrator).

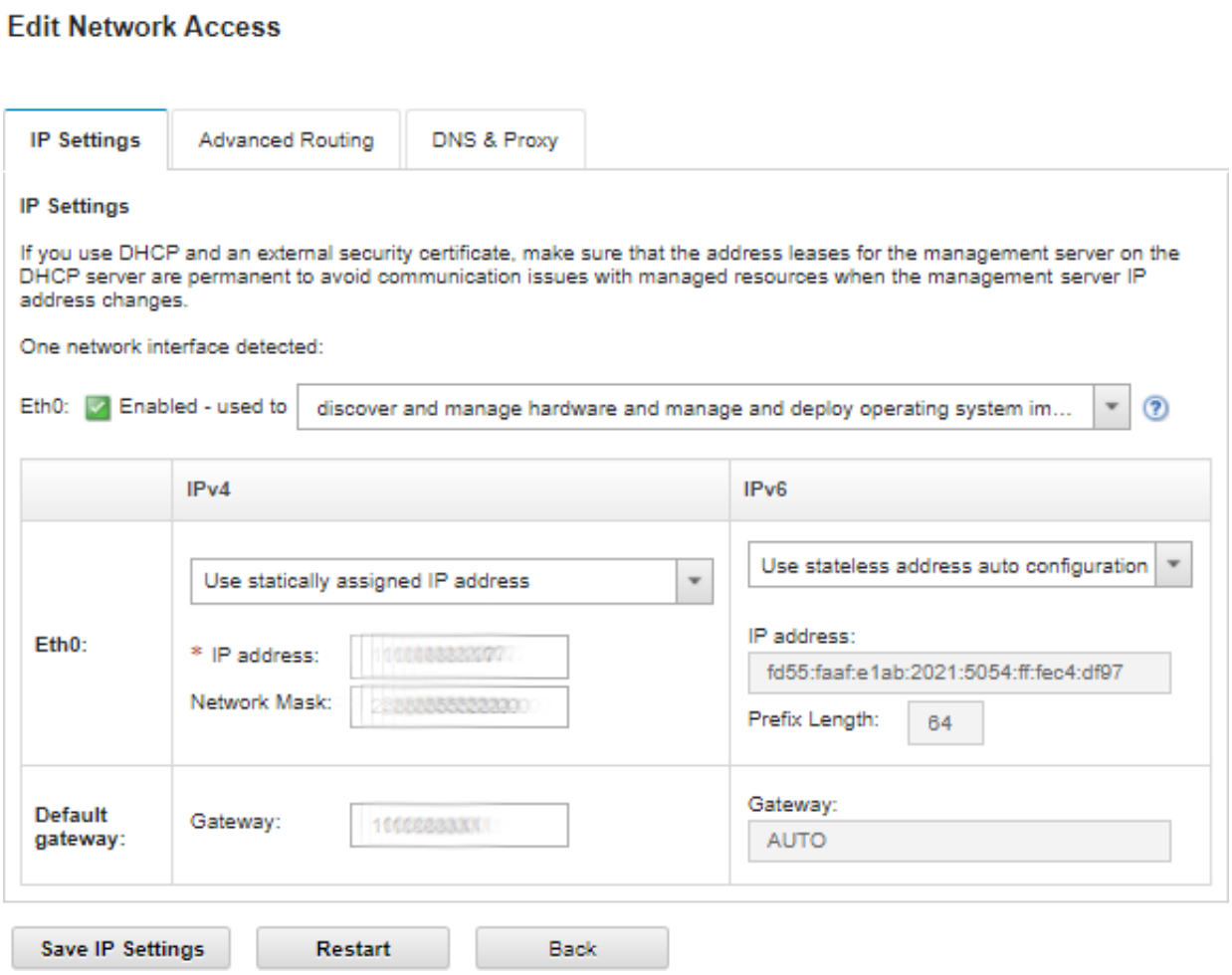
Vulnerabilidades do Samba e do Apache

O Lenovo XClarity Administrator usa servidores Samba e Apache como um compartilhamento remoto somente leitura ao implantar o sistema operacional e atualizar drivers de dispositivo do SO. Se você não pretende usar o XClarity Administrator para gerenciar sistemas operacionais, é possível desativar os servidores Samba e Apache definindo a função de rede do XClarity Administrator para descobrir e gerenciar somente o hardware.

Procedimento

Para desativar servidores Samba e Apache, conclua as etapas a seguir.

1. Na barra de menus do XClarity Administrator, clique em **Administração → Acesso à Rede**. As configurações de rede definidas atualmente são exibidas.
2. Clique em **Acesso à rede** para exibir a página Editar Acesso à Rede.



3. Selecione a opção **descobrir e gerenciar somente hardware** para a interface de rede.
4. Clique em **Salvar configurações de IP**.
5. Clique em **Reiniciar** para reiniciar o servidor de gerenciamento.

Capítulo 11. Solução de problemas de backup e restauração

Use estas informações para solucionar problemas de backup e restauração.

O processo de backup parece ter sido interrompido durante a reinicialização do servidor de gerenciamento

Gerar um backup do Lenovo XClarity Administrator pode levar alguns minutos. Uma barra de progresso mostra o status do trabalho.

Procedimento

Se o processo backup parecer ter sido interrompido, conclua as etapas a seguir.

- Se o botão **Cancelar** ficar visível, você poderá cancelar o processo de backup.
- Se o botão **Cancelar** não ficar visível, abra uma nova guia para ver se o botão **Cancelar** é exibido.
- Se isso não resolver o problema, reinicie a máquina virtual.

Nota: Se você cancelar o processo de backup ou reinicializar a máquina virtual, um backup poderá não ser criado.

A janela do XClarity Administrator fica em branco após a atualização durante o backup

O Lenovo XClarity Administrator será fechado durante o procedimento para impedir que os dados sejam modificados. Se você atualizar ou fechar a janela do XClarity Administrator antes que o processo de backup seja concluído e que o servidor de gerenciamento seja reiniciado, a janela do XClarity Administrator poderá aparecer em branco se o servidor de gerenciamento ainda estiver em modo desativado.

Procedimento

Conclua as seguintes etapas para resolver esse problema.

1. Atualize a página periodicamente para verificar se ela carrega.
2. Se a janela permanecer em branco após um período considerável, reinicie a máquina virtual.
3. Se ele ainda não for carregado, exclua manualmente o arquivo `/opt/lenovo/lxca/bin/QUIESCE_MODE_FLAG`.

   Nota: Esta etapa requer acesso raiz. Entre em contato com o suporte antes de executar esta etapa.
4. Reinicie a máquina virtual do XClarity Administrator.

© Copyright Lenovo 2015, 2025

Capítulo 12. Problemas de monitoramento e transmissão de evento

Use estas informações para solucionar problemas de monitoramento e encaminhamento de eventos.

Os eventos não são encaminhados

Use estas informações para solucionar problemas ao encaminhar eventos.

- Se uma programação for criada para o encaminhador de evento, apenas os eventos que ocorrerem durante o período programado serão encaminhados. Verifique se o período programado não passou.
- Para serviços da Web baseados em e-mail:
  - Se um tipo de conexão segura for selecionado para o encaminhador de eventos, o Lenovo XClarity Administrator tentará baixar e importar o certificado do servidor SMTP para seu armazenamento confiável. Você é solicitado a aceitar a adição desse certificado ao armazenamento confiável. Se isso falhar, a conexão com o servidor SMTP não é possível.

    Para resolver esse problema, importe o certificado manualmente para o XClarity Administrator clicando em **Administração → Segurança → Certificados confiáveis** e no ícone **Criar** ( ).
  - Verifique se o servidor SMTP aceita somente e-mails que foram enviados por um usuário registrado. Se esse for o caso, o endereço do remetente padrão (`LXCA.`*<source_identifier>*`@`*<smtp_host>*) será rejeitado. Para resolver o problema, especifique pelo menos um nome de domínio no campo **Do endereço** no encaminhador de eventos.
  - Se estiver usando a autenticação OAUTH2, verifique se o token de segurança não expirou. Se estiver expirado, o script Python do oauth2.py e o token de atualização para gerar um novo token de segurança. Em seguida, atualize o encaminhador de eventos no XClarity Administrator com o novo token de segurança. Para obter mais informações, consulte Configurando o encaminhamento de evento em um serviço SMTP do Gmail.

© Copyright Lenovo 2015, 2025

Capítulo 13. Problemas de gerenciamento de dispositivos

Use estas informações para solucionar problemas de gerenciamento de dispositivos e operação.

Não é possível apagar com segurança os dados em unidades paralisadas

Use essas informações para solucionar problemas quando ocorre uma falha de apagamento seguro em unidades de disco rígido SATA com o erro `Os discos estão paralisados e não podem ser apagados.`

As unidades de disco rígido SATA internas estão no estado paralisado por padrão. Se o servidor tiver uma unidade paralisada, o Lenovo XClarity Administrator reativará temporariamente a unidade paralisada e, em seguida, inicializará a Bare Metal Update (BMU) para apagar a unidade. Quando a XClarity Administrator BMU é interrompida e o servidor é inicializado no sistema operacional, a unidade fica paralisada novamente automaticamente.

Quando um servidor é gerenciado no XClarity Administrator usando o modo de *autenticação gerenciada*, o XClarity Administrator cria a conta LDAP SYSMGR_xxx para gerenciar e monitorar o servidor em vez das credenciais locais (consulte Gerenciando o servidor de autenticação na documentação online do XClarity Administrator). A conta LDAP SYSMGR_xxx não tem um privilégio IPMI, portanto, o XClarity Administrator não pode reativar o disco, fazendo com que a operação de apagamento seguro falhe nesse servidor.

Para resolver esse problema, gerencie o servidor usando o modo de *autenticação local* e, em seguida, tente apagar com segurança as unidades.

Não é possível apagar com segurança volumes SDD SATA quando conectados ao Marvel RAID

Use essas informações para solucionar problemas quando ocorre uma falha no apagamento seguro em SDDs SATA com volumes quando conectados aos controladores Marvell RAID.

Não é possível apagar com segurança volumes SDD SATA conectados aos controladores RAID da Marvell. Em vez disso, considere as seguintes recomendações.

- Para SSDs SATA de 7 mm, conecte-se aos controladores Broadcom RAID para executar o apagamento seguro.
- Para SSDs SATA M.2, conecte-se a controladores Marvell não RAID (como o Kit de ativação de dois compartimentos ThinkSystem M.2 SATA/NVMe) para realizar o apagamento seguro.

Há um tempo limite interno (9 segundos) no firmware do Marvell RAID. Se o SSD não responder ao comando a tempo (não concluir o apagamento), o firmware Marvell RAID vai reconfigurar o SDD, o SDD será bloqueado e ocorrerá uma falha no apagamento seguro. Para desbloquear o SDD, execute o comando a seguir.

```
hdparm --user-master u --security-unlock user123 %diskName%
```

Os dados do inventário não são atualizados depois de adicionar ou substituir placas

Para dispositivos baseados em AMD1P e TSM, o Lenovo XClarity Administrator pode não exibir dados corretos do inventário, como FRU e firmware, para placas PCIe recém-inseridas.

© Copyright Lenovo 2015, 2025

Depois de alterar uma placa PCIe, você deve reiniciar o dispositivo gerenciado e aguardar alguns minutos para que o Baseboard Management Controller atualize o inventário.

O XClarity Administrator busca automaticamente dados do inventário de dispositivos gerenciados a cada 24 horas. É possível aguardar a próxima coleta de inventário ou coletar manualmente os dados do inventário selecionando o servidor na página Servidor e, em seguida, clicando em **Ações → Inventário → Atualizar Inventário**.

Capítulo 14. Problemas de configuração do servidor

Use estas informações para solucionar problemas com padrões e perfis do servidor.

Ocorre um erro ao criar um padrão de um servidor existente

Use estas informações para solucionar problemas ao criar padrões de um servidor gerenciado existente.

1. Certifique-se de que o status do servidor não seja Offline. Para obter mais informações sobre padrões de servidor, consulte Criando um padrão de servidor na documentação online do Lenovo XClarity Administrator.
2. Repita a operação.

Ao implantar um padrão em um dispositivo, ocorre um erro de ativação

Um erro de ativação indica que ocorreu um problema ao implantar o padrão de servidor em um dispositivo gerenciado. Um erro de ativação pode ocorrer por diversos motivos. Use estas informações para solucionar esses tipos de problemas.

Revise os detalhes do trabalho na página Trabalhos. Para isso, localize o trabalho de ativação do perfil de servidor com o status "Interrompido com Erros" e clique no trabalho. Para identificar o problema, revise as mensagens de erro.

- Problemas de conectividade ou roteamento de rede entre o Lenovo XClarity Administrator e o dispositivo gerenciado.

  Esses problemas podem ser representados nas mensagens de trabalho como erros LDAP. Isso indica que houve um problema relacionado à conexão do dispositivo ao dispositivo virtual por uma das interfaces de rede configuradas.

  Verifique se a conexão de rede entre o dispositivo virtual do XClarity Administrator e o dispositivo está operacional. Se eles estiverem em segmentos de rede diferentes, certifique-se de que haja roteabilidade da rede entre os dois segmentos.
- Uma ou mais definições de configuração no padrão de servidor resultam em uma alteração de configuração que não é válida no dispositivo gerenciado selecionado. Considere os exemplos a seguir.
  - O padrão de UEFI estendida selecionado não é compatível com o dispositivo selecionado.

    Por exemplo, se um padrão UEFI fornecido com o XClarity Administrator para um servidor baseado em X6 (como o System x3950 X6) estiver selecionado e implantado em um servidor System x3650 M4, as diferenças nas configurações do processador entre os dois servidores poderão causar falha na ativação do perfil. Para resolver o problema, certifique-se de que o padrão UEFI estendido selecionado seja compatível com o servidor selecionado.
  - Um padrão de porta para uma porta de adaptador Ethernet é atribuído a uma porta que não oferece suporte às configurações selecionadas.

    Por exemplo, em adaptadores baseados em Emulex, há configurações que são expostas apenas na primeira porta do adaptador, especificamente o Modo Avançado e as configurações de porta que são usadas para desabilitar uma porta. Se essas configurações forem atribuídas à segunda porta do adaptador, poderá ocorrer um erro de ativação. Esses problemas podem ser representados nas mensagens do trabalho como `AdvancedMode não é uma configuração` ou `Port1 não é uma configuração`. Para resolver esse problema, assegure-se de que o padrão de porta que inclui essas configurações de Padrão de Porta Estendida para Modo Avançado ou Ativação de Porta seja atribuído apenas à primeira porta do adaptador.

© Copyright Lenovo 2015, 2025

– Algumas configurações não são permitidas no dispositivo gerenciado selecionado após uma atualização de firmware.

  Por exemplo, depois de atualizar o firmware de um adaptador de E/S, algumas configurações podem ser removidas ou renomeadas pelo novo firmware e, portanto, a configuração no padrão de servidor pode não ser válida no servidor de destino. Esses problemas são representados na mensagem de trabalho como "xxx não é uma configuração". Para resolver esse problema, você pode aprender um novo padrão de servidor do servidor para que o novo padrão inclua todas as configurações compatíveis com o novo firmware. Se você precisar continuar usando o padrão antigo, edite manualmente o padrão de servidor para remover as configurações inválidas.

- Ocorre um erro ao ligar ou reiniciar o servidor quando a Ativação Completa está selecionada para a implantação do padrão ou do perfil

  Certifique-se de que o estado de energia do dispositivo esteja declarado corretamente no XClarity Administrator. Se não estiver, atualize o inventário para sincronizar o estado de energia:

  1. Na barra de menu do XClarity Administrator, clique em **Hardware → Servidores**. A página Servidores é exibida com uma exibição tabular de todos os servidores gerenciados (servidores de rack e nós de cálculo).
  2. Selecione o servidor e clique em **Todas as Ações → Atualizar Inventário**.

Uma configuração inválida foi implantada em um comutador

Use estas informações para solucionar problemas quando uma configuração inválida for implantada em um comutador

É necessário criar IDs de VLAN antes de adicionar uma porta a uma VLAN específica. Se um padrão da porta tiver configurações de VLANs de porta interna do comutador com IDs de VLAN que não foram pré-configurados para o comutador, a ativação do perfil talvez não seja bem-sucedida, mas a configuração inválida e não aplicada no comutador deve ser reparada.

Para resolver esse problema, faça login no comutador e configure manualmente os pré-requisitos, ou desfaça as alterações implantando um padrão com configurações válidas.

Capítulo 15. Problemas de repositório e atualização de firmware

Use estas informações para solucionar problemas de atualização de firmware.

Falha ao conectar-se ao repositório Lenovo

O Lenovo XClarity Administrator v2.8 e anteriores usam uma conexão HTTP com o Suporte Lenovo para atualizar o catálogo de atualizações de firmware e baixar pacotes de atualização; no entanto, o Suporte Lenovo agora requer uma conexão HTTPS.

Instale o GAFix mais recente em sua instância do XClarity Administrator ou faça a atualização para o XClarity Administrator v3.0.0 ou posterior.

Após a atualização de firmware, a página Aplicar/Ativar não mostra versões do firmware atualizadas

Use estas informações para solucionar problemas com a página Atualizações de Firmware: Aplicar/Ativar.

Verifique se o inventário mais recente está sendo comparado clicando no ícone **Atualizar** ( ) na página Atualizações de Firmware: Aplicar/Ativar para solicitar uma sincronização com os dados do dispositivo Lenovo XClarity Administrator.

Não é possível atualizar o firmware em um dispositivo

Use estas informações para solucionar problemas ao atualizar o firmware nos dispositivos gerenciados.

- Revise Considerações de atualização de firmware na documentação online do XClarity Administrator e siga as recomendações fornecidas.
- Certifique-se de que o status do servidor não é Offline e que o dispositivo possa ser detectado na rede do Lenovo XClarity Administrator.
- Se você encontrar um problema ao atualizar o firmware em um comutador FC5022 executando o FOS v7.4.x e anterior, execute o seguinte comando em uma interface da linha de comando. Para obter mais informações, consulte Dicas técnicas HT507915.

```
Seccrypto -- default -type SSH -force
```

A atualização de firmware do CMM trava

Use estas informações para resolver problemas ao atualizar o firmware do CMM, pilha Flex versão 1.3.2.1 2PET12K a 2PET12Q, em execução por mais de três semanas e que faz parte de uma configuração dupla do CMM.

1. Execute um reposicionamento virtual do CMM. Se você tiver dois CMMs no mesmo chassi, reposicione virtualmente os dois CMMs simultaneamente. É possível localizar os níveis mínimos de firmware necessários em Página da Web Suporte do XClarity Administrator – Compatibilidade clicando na guia **Compatibilidade** e, em seguida, clicando no link para os tipos de dispositivo apropriados.
2. Execute a atualização novamente no XClarity Administrator.

© Copyright Lenovo 2015, 2025

O firmware está atualizado, mas não realiza a verificação de conformidade

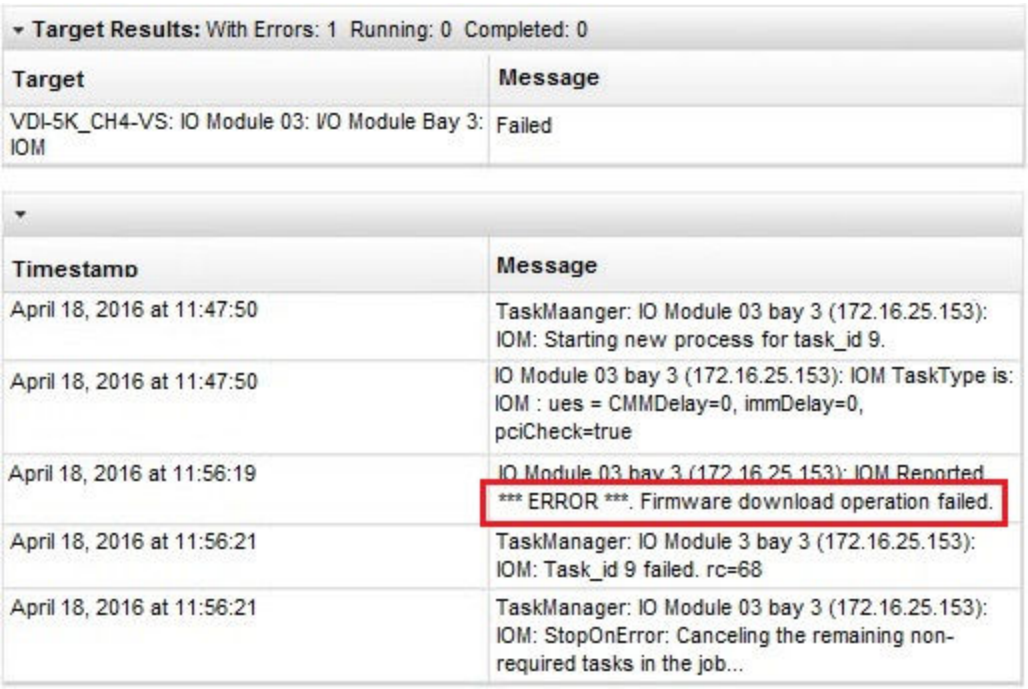
Use estas informações para solucionar problemas de conformidade depois de uma atualização de firmware.

Execute um reposicionamento virtual no dispositivo ou execute uma atualização adicional, como uma atualização de HDD.

Atualizações de firmware em comutadores Flex System falham inesperadamente

Os tópicos a seguir descrevem erros que podem ser encontrados no log de trabalhos.

Para localizar as mensagens, clique em **Monitoramento → Trabalhos** no menu Lenovo XClarity Administrator. Para localizar a mensagem de erro, clique no link do trabalho na coluna **Trabalhos** para exibir a caixa de diálogo de resumo de trabalhos e resultados. Na seção Resultados Desejados, a mensagem está listada na coluna **Mensagem** e começa com `"***ERRO***`.



Target Results: With Errors: 1 Running: 0 Completed: 0

Target	Message
VDI-5K_CH4-VS: IO Module 03: I/O Module Bay 3: IOM	Failed

Timestamp	Message
April 18, 2016 at 11:47:50	TaskMaanger: IO Module 03 bay 3 (172.16.25.153): IOM: Starting new process for task_id 9.
April 18, 2016 at 11:47:50	IO Module 03 bay 3 (172.16.25.153): IOM TaskType is: IOM : ues = CMMDelay=0, immDelay=0, pciCheck=true
April 18, 2016 at 11:56:19	IO Module 03 bay 3 (172.16.25.153): IOM Reported *** ERROR ***. Firmware download operation failed.
April 18, 2016 at 11:56:21	TaskManager: IO Module 3 bay 3 (172.16.25.153): IOM: Task_id 9 failed. rc=68
April 18, 2016 at 11:56:21	TaskManager: IO Module 03 bay 3 (172.16.25.153): IOM: StopOnError: Canceling the remaining non-required tasks in the job...

Importante: Atualizações de firmware do comutador Flex usando XClarity Administrator podem falhar de forma intermitente. Em caso de falhas, experimente as sugestões nos tópicos a seguir. Se as atualizações de firmware do comutador Flex continuarem a falhar usando o XClarity Administrator, atualize os comutadores Flex diretamente da interface do comutador Flex.

Nota: As atualizações de firmware em um comutador Flex System poderão falhar inesperadamente se o comutador não estiver executando EHCM L3. Para obter mais informações, consulte Considerações de atualização de firmware na documentação online do XClarity Administrator.

A atualização de firmware no comutador Flex falhou, indicando um erro com a mensagem "Falha na operação de download de firmware."

Use estas informações para solucionar problemas de uma mensagem de erro `O IOM relatou ***ERRO*** Falha na operação de download de firmware` no log de trabalhos. Isso poderá ocorrer nos comutadores EN4023 e FC5022 se você estiver tentando realizar uma atualização prejudicial que requer ignorar uma versão de atualização de firmware anterior e pular diretamente para a mais recente.

Para solucionar esse problema, atualize o comutador Flex diretamente na interface da Web ou na CLI do comutador Flex.

Para o FC5022, a migração de FOS v7.3 para v8.0.1-pha é uma atualização que gera transtornos. A migração de FOS v7.4 para FOS v8.0.1-pha é uma atualização que não gera transtornos.

É possível localizar os níveis mínimos de firmware necessários em Página da Web Suporte do XClarity Administrator – Compatibilidade clicando na guia **Compatibilidade** e, em seguida, clicando no link para os tipos de dispositivo apropriados.

A atualização de firmware no comutador Flex falhou, indicando um erro com a mensagem "DCSS_RC_CDT_FAIL"

Use estas informações para solucionar problemas de uma mensagem de erro `IOM: Relatado o ***ERRO*** DCSS_RC_CDT_FAIL` no log de trabalhos. Isso indica que o comutador Flex pode estar desligado ou apresentando algum outro problema de comunicação.

Execute as seguintes ações nesta ordem. Depois de cada etapa, tente atualizar o firmware novamente.

1. Verifique se o comutador Flex está ligado.
2. Verifique se o comutador Flex tem um endereço IP válido.
3. Redefina o comutador Flex.
4. Redefina/reinicie o CMM.

A atualização de firmware no comutador Flex falhou, indicando um erro com a mensagem de "tempo limite"

Use estas informações para solucionar problemas de uma mensagem de erro `IOM: Relatado o ***ERRO*** tempo limite` no log de trabalhos. Isso poderá ocorrer se o endereço IP do comutador não estiver acessível na rede no Lenovo XClarity Administrator.

Execute as seguintes ações nesta ordem. Depois de cada etapa, tente atualizar o firmware novamente.

1. Garanta que o comutador Flex tenha um endereço IP válido e esteja acessível na rede no XClarity Administrator.
2. Redefina o comutador Flex.
3. Redefina/reinicie o CMM.

A atualização de firmware no comutador Flex falhou, indicando um erro com a mensagem "Não é possível baixar a mesma versão do firmware. Baixe outro firmware."

Use estas informações para solucionar problemas de um `IOM: Relatou ***ERRO*** Não é possível baixar a mesma versão do firmware. Baixe outro firmware.` mensagem de erro no log de trabalhos. Isso poderá ocorrer se você estiver tentando atualizar o EN4023 para o mesmo nível.

O EN4023 não permite a atualização do firmware para o mesmo nível que já está em execução.

A atualização de firmware no comutador Flex falhou, indicando um erro com a mensagem de falha ao contatar o host

Use estas informações para solucionar problemas de uma mensagem de erro IOM: Relatado o ***ERRO*** Falha ao contatar o host no log de trabalhos. Isso poderá ocorrer se o endereço IP do comutador não estiver acessível na rede no Lenovo XClarity Administrator.

Execute as seguintes ações nesta ordem. Depois de cada etapa, tente atualizar o firmware novamente.

1. Garanta que o comutador tenha um endereço IP válido e esteja acessível na rede no XClarity Administrator.
2. Reinicie o comutador.
3. Reinicie o CMM.

A atualização de firmware no comutador Flex falhou, indicando um erro com a mensagem "o arquivo não existe"

Use estas informações para solucionar problemas de uma mensagem de erro `IOM: Relatado o ***ERRO*** O arquivo não existe` no log de trabalhos. Isso poderá ocorrer se o endereço IP do comutador não estiver acessível na rede no Lenovo XClarity Administrator.

Execute as seguintes ações nesta ordem. Depois de cada etapa, tente atualizar o firmware novamente.

1. Garanta que o comutador tenha um endereço IP válido e esteja acessível na rede no XClarity Administrator.
2. Reconfigure o comutador.
3. Redefina/reinicie o CMM.

A atualização de firmware no comutador Flex falhou, indicando um erro com a mensagem "falha quando a luz para de piscar"

Use estas informações para solucionar problemas de uma mensagem de erro `IOM: Relatado o ***ERRO*** Falha quando a luz para de piscar` no log de trabalhos. Isso poderá ocorrer se o comutador não tiver um endereço IP válido.

Garanta que o comutador tenha um endereço IP válido e esteja acessível na rede no Lenovo XClarity Administrator.

Falha inesperada na atualização de firmware no Comutador Ethernet de 40 Gb EN6131 ou no Comutador InfiniBand IB6131

Use estas informações para solucionar uma falha inesperada ao atualizar o firmware do comutador EN6131 40 Gb Ethernet Switch ou IB6131 InfiniBand Switch.

1. Verifique no log de trabalho se há uma mensagem de erro do comutador, como `Não há espaço em disco suficiente para baixar a imagem.`

   Nota: Pode haver informações adicionais no log de trabalhos. Em geral, o formato é `IOM: Relatado o *** ERRO ***` *msg*, onde *msg* é o erro específico para esse módulo.
2. Verifique a velocidade e a estabilidade da rede. Poderá ocorrer falha no firmware se a atualização não for concluída em até 30 minutos.
3. Libere espaço em disco suficiente no comutador para o arquivo de atualização. O espaço em disco é usado ao copiar os arquivos de atualização no comutador. Consulte Comutador Ethernet de 40 GB Lenovo Flex System EN6131 na documentação online do Flex Systems para obter instruções de gerenciamento do espaço em disco.

4. Execute a atualização novamente no Lenovo XClarity Administrator.

Falha na atualização de firmware no módulo intermediário Lenovo EN4091

Use estas informações para solucionar uma falha inesperada ao atualizar o firmware do módulo intermediário Lenovo EN4091.

1. Verifique no log de trabalhos se há uma mensagem de erro do módulo intermediário, como `Falha na verificação de integridade de dados na imagem de firmware` ou `Falha ao contatar o host`.

   Nota: Pode haver informações adicionais no log de trabalhos. Em geral, o formato da mensagem é `IOM: Relatado o *** ERRO *** msg`, onde *msg* é o erro específico para esse módulo.
2. Execute um reposicionamento virtual do Lenovo EN4091.
3. Execute a atualização novamente no Lenovo XClarity Administrator.

A atualização de firmware no comutador Flex System falhou, indicando um erro com a mensagem "Falha de autenticação da chave do host"

Uma mensagem de erro no log de trabalhos no formato "IOM: Relatado o ***ERRO*** Falha de autenticação da chave do host" é exibida. Isso acontece quando a chave SFTP é alterada em um servidor SFTP que era usado antes da atualização do comutador Flex System. Os comutadores afetados são: CN4093, EN2092, EN4091, EN4093, EN4093R, SI4093.

No Lenovo XClarity Administrator, esse erro poderá ocorrer se você atualizar o firmware em um comutador Flex System e, depois, instalar outra versão posterior do XClarity Administrator ou reinicializar o XClarity Administrator e tentar atualizar o comutador em seguida. Isso ocorre porque a instalação de uma nova versão do XClarity Administrator ou a reinicialização do XClarity Administrator pode fazer com que uma nova chave SFTP seja gerada.

Para resolver esse problema, insira o comando a seguir na CLI de um comutador Flex System ou um comutador Lenovo Flex System para limpar as chaves SSH. Observe que, se o comutador usar ISCLI, você deverá estar no modo Terminal de Configuração para executar o comando. É possível alterar o modo Terminal de Configuração executando o comando `enable` e, em seguida, o comando `configure terminal`.

```
clear ssh-clienthostkey all
```

Nota: Se o comutador Flex System estiver no modo de IBMNOS CLI, insira os seguintes comandos na CLI do comutador para limpar as chaves SSH:

```
maint
clssh
all
exit
```

Ao executar uma atualização, o sistema não entra no modo de manutenção

Use estas informações para solucionar problemas com atualizações de firmware e modo de manutenção.

Repita a atualização de firmware.

Reiniciar um servidor do sistema operacional não ativa o modo de manutenção

Ao atualizar o firmware com ativação atrasada em qualquer um dos servidores a seguir, o status de atualização mostra "Modo de manutenção pendente" mesmo após a reinicialização do servidor no sistema operacional.

- Flex System x240 M5, Tipos 2591 e 9532
- NeXtScale nx360 M5, Tipo 5465
- System x3250 M6, Tipos 3633 e 3943
- System x3550 M5, Tipo 5463
- System x3500 M5, Tipo 5464
- System x3550 M5, Tipo 8869
- System x3650 M5, Tipo 5462
- System x3650 M5, Tipo 8871

Para resolver esse problema, reinicie o servidor na interface da Web do controlador de gerenciamento. Quando o servidor estiver novamente online, o processo de ativação da atualização será retomado.

O servidor executando o Red Hat Enterprise Linux (RHEL) não reinicia

Para o Red Hat® Enterprise Linux (RHEL) v7 e posterior, reiniciar o sistema operacional partindo de um modo gráfico suspende o servidor por padrão.

Configure manualmente o RHEL para alterar o comportamento do botão de energia para desligar. Para obter instruções, consulte o Guia de administração e migração de dados Red Hat: Mudar o comportamento ao pressionar o botão de ligar no modo de destino gráfico .

Capítulo 16. Problemas de repositório e atualização de driver de dispositivo do SO

Use estas informações para solucionar problemas de atualização de driver de dispositivo do SO.

Não é possível se conectar ao site de suporte da Lenovo para baixar atualizações de drivers de dispositivo

Use estas informações para solucionar problemas ao baixar UpdateXpress System Packs (UXSPs) e os drivers de dispositivo do site de suporte da Lenovo.

- Verifique se a porta do dispositivo Lenovo XClarity Administrator (eth0 ou eth1) que está configurada para gerenciamento tem acesso à Internet. Para obter mais informações sobre considerações de rede, consulte Considerações de rede na documentação online do XClarity Administrator.
- Verifique se todas as portas e os endereços de internet necessários que estão disponíveis antes de tentar atualizar os drivers de dispositivo em um servidor gerenciado. Para obter mais informações sobre portas, consulte Disponibilidade de porta e Firewalls e servidores proxy na documentação online do XClarity Administrator.

Não é possível atualizar drivers de dispositivo em um servidor

Use estas informações para solucionar problemas ao atualizar drivers de dispositivo em um servidor gerenciado.

- Certifique-se de que o servidor esteja online e acessível na rede no Lenovo XClarity Administrator.
- Revise as considerações sobre atualização de driver de dispositivo (consulte Considerações sobre atualização de drivers de dispositivo do SO na documentação online do XClarity Administrator).

© Copyright Lenovo 2015, 2025

Capítulo 17. Problemas de implantação do sistema operacional

Use estas informações para solucionar problemas que você possa encontrar ao tentar implantar sistemas operacionais em servidores gerenciados no Lenovo XClarity Administrator.

Para problemas gerais relacionados à implantação do sistema operacional, consulte Não é possível implantar um sistema operacional.

Problemas no relatório de status durante a implantação do SO

Use estas informações para solucionar problemas no relatório de status pelo Lenovo XClarity Administrator durante a implantação do sistema operacional.

- Ao implantar o VMware 6.5 ou posterior usando o XClarity Administrator v1.4.0 e anterior, o status do trabalho pode relatar que a implantação está concluída antes que o sistema operacional esteja pronto.

  Ao usar scripts para monitorar a conclusão da implantação do SO, adicione um atraso de 10 minutos para o script depois de receber o status do trabalho de implantação indicando que a implantação do SO foi concluída.
- Ao implantar o Windows em uma rede que usa a marcação de VLAN, erros de status podem ser relatados durante a *passagem de specialize configuração* da implantação.

  Você pode ignorar esses erros.

Não é possível implantar um sistema operacional

Use estas informações para solucionar problemas gerais que você possa encontrar ao tentar implantar um sistema operacional em um servidor gerenciado no Lenovo XClarity Administrator.

Em ambientes de rede lentos, a implantação do sistema operacional do SLES 12 e 12.1 em modo IP estático poderá falhar porque o parâmetro de inicialização de atraso de rede não entrará em vigor nesse modo. Esse problema é corrigido no SLES 12.2.

Conclua as etapas a seguir para resolver o problema:

1. Para Servidores ThinkSystem V3 e V4 (com XCC2 ou XCC3) que tenham o protetor do sistema habilitado e a ação definida para **Impedir a inicialização do SO**, o protetor do sistema deve ser compatível com o dispositivo. Se o protetor do sistema não for compatível, os dispositivos serão impedidos de concluir o processo de inicialização, o que faz com que a implantação do SO falhe. Para provisionar esses dispositivos, responda manualmente ao prompt de inicialização do protetor do sistema para permitir que os dispositivos seja inicializados normalmente.
2. Se você vir a mensagem `https://<management_server_IP>/osdeployment/connection/... Permissão negada`, atualize o BIOS no servidor e altere a configuração de data e hora para a data e a hora atuais.
3. Revise todos os requisitos para o sistema operacional que está sendo implantado. Consulte Sistemas operacionais suportados na documentação online do XClarity Administrator.Exemplo:
   - Poderá ocorrer um problema na implantação do VMware ESXi se você não configurar o espaço de E/S de mapeada em memória (MMIO) para pelo menos 3 GB.
   - Se você estiver implantando o Microsoft Windows e ingressando em um domínio do Active Directory, siga as considerações descritas em Integração com Windows Active Directory na documentação online do XClarity Administrator.

© Copyright Lenovo 2015, 2025

4. Revise as limitações do suporte de implantação do sistema operacional para adaptadores de E/S específicos. Para obter mais informações sobre o suporte a adaptadores de E/S, consulte Página da Web Suporte do XClarity Administrator – Compatibilidade.
5. Certifique-se de que você tenha uma conexão de rede estável entre o XClarity Administrator e o dispositivo (servidor gerenciado) em que o sistema operacional será instalado.

   Nota: Ao implantar o SLES 11 SP4, a implantação poderá parar e não reiniciar se a conexão de rede for perdida entre o XClarity Administrator e o dispositivo. Se isso ocorrer, verifique seu ambiente de rede e reimplante o sistema operacional.
6. Certifique-se de que pelo menos uma porta de rede XClarity Administrator seja definida para gerenciar e implantar imagens do sistema operacional.É possível configurar a topologia de rede XClarity Administrator na página Acesso à Rede. Para obter mais informações sobre a página Acesso à Rede, consulte Configurando o acesso à rede na documentação online do XClarity Administrator.
7. Verifique se a porta de rede do XClarity Administrator que está sendo usada para conexão à rede de dados está configurada para estar na mesma rede que as portas de rede de dados no servidor gerenciado. A porta do servidor é especificada pelo endereço MAC e pode ser configurada por meio da página Sistemas Operacionais - > Configurações de Rede. Para obter mais informações sobre a edição de configurações de rede, consulte Definindo as configurações de rede para servidores gerenciados na documentação online do XClarity Administrator.
8. Certifique-se de que o servidor de destino não tenha um padrão de servidor adiado ou ativado parcialmente. Se um padrão de servidor foi adiado ou ativado parcialmente no servidor de destino, reinicie o servidor para aplicar todas as definições de configuração.
9. Veja o status do servidor na página Implantar Imagens de SO para assegurar que ele tenha um status de implantação "Pronto". Se o status for "Não Pronto", clique no link de status para determinar por que o servidor não está pronto para a implantação do sistema operacional.Para obter mais informações sobre implantação do sistema operacional, consulte Implantando uma imagem do sistema operacional na documentação online do XClarity Administrator.
10. Verifique se o dispositivo tem visibilidade do local de armazenamento que foi selecionado para a implantação do sistema operacional.

    Dica: Para garantir que as implantações do sistema operacional sejam bem-sucedidas, remova todo o armazenamento do servidor gerenciado, exceto o armazenamento escolhido para a implantação do sistema operacional.

Não é possível importar um arquivo para o repositório de imagens do SO

Use esta seção de informações para solucionar problemas que você possa encontrar ao tentar importar arquivos para o repositório de imagens do Lenovo XClarity Administrator.

Conclua as etapas a seguir para resolver o problema:

- Certifique-se de que o arquivo que está sendo importado tenha sido verificado por meio do teste de soma de verificação.
- Verifique se o sistema operacional base a seguir é compatível com o XClarity Administrator. Consulte Sistemas operacionais suportados na documentação online do XClarity Administrator.
- Se você estiver importando do sistema local:
  - Os navegadores da Web Internet Explorer e Microsoft Edge têm um limite de upload de 4 GB. Se o arquivo que você está importando for maior que 4 GB, considere usar outro navegador da Web (como o Chrome ou o Firefox)
- Se estiver importando de um servidor de arquivos remoto:
  - Verifique se o caminho completo para o arquivo corresponde ao caminho real no servidor de arquivos remoto.

- Verifique se o caminho completo para o arquivo contém as barras comuns ou inversas corretas, dependendo do sistema operacional que está hospedando o servidor de arquivos remoto.
- Verifique se as permissões necessárias foram concedidas ao diretório no servidor de arquivos remoto.
- Verifique se há espaço em disco suficiente no repositório de imagens do SO para armazenar o arquivo (consulte Gerenciando espaço em disco na documentação online do XClarity Administrator).
- Verifique se você está conectado ao servidor de arquivos remoto usando as credenciais corretas.
- Verifique se você tem uma conexão de rede estável entre o XClarity Administrator e o servidor de arquivos remoto.
- Verifique se os certificados confiáveis corretos foram importados e se os certificados não foram revogados (consulte Trabalhando com certificados de segurança na documentação online do XClarity Administrator).
- Verifique se o servidor de arquivos remoto oferece suporte a pelo menos um algoritmo que seja compatível com o XClarity Administrator para cada tipo de algoritmo exigido pelo SSH (consulte Implementando um ambiente seguro na documentação online do XClarity Administrator).

O instalador do SO não pode localizar a unidade de disco em que você deseja instalar

Para servidores que incluem adaptadores RAID de software (como o Adaptador AnyRAID 110i, o adaptador ServeRAID C100 ou C105 e o adaptador RAID Intel RSTe SATA Software), quando o adaptador SATA é habilitado no controlador de gerenciamento, o modo SATA deve ser definido como "AHCI". Outros modos (como "RAID" e "IDE") não são aceitos para RAID de software pelos sistemas operacionais RHEL, SUSE, VMware ou Windows.

Nota: Cada servidor deve ter um adaptador RAID de hardware instalado e configurado. O RAID do software que geralmente está presente no adaptador de armazenamento Intel SATA integrado não é suportado. No entanto, se um adaptador RAID de hardware não estiver presente, a configuração do adaptador SATA no modo AHCI SATA ativado para implantação do sistema operacional poderá funcionar em alguns casos.

Para modificar o modo SATA para ThinkServers, conclua as etapas a seguir.

1. No AMI Setup Utility, selecione o menu **Configurações Avançadas**.
2. Use as teclas de seta para selecionar o **SATA Mode**.
3. Pressione **+** para alterar o valor para `AHCI`.
4. Pressione **F10** para salvar a alteração.

Para modificar o modo SATA para outros servidores, conclua as etapas a seguir.

1. No F1 Setup Utility, selecione o menu **Configurações do Sistema → Dispositivos e Portas de E/S → Modo SATA Integrado**.
2. Pressione **+** para alterar o valor para `AHCI`.
3. Pressione **F10** para salvar a alteração.

O instalador do SO não pode inicializar em um servidor ThinkServer

Para os servidores ThinkServer, a Política de OpROM de Armazenamento no Módulo de Gerenciamento ThinkServer deve ser definida como "UEFI Only" para que a imagem do instalador do SO seja inicializada corretamente. Se a política estiver definida como "Legacy Only", o instalador do SO não será inicializado.

Para modificar a Política de OpROM de Armazenamento, conclua as etapas a seguir.

1. No AMI Setup Utility, selecione o menu **Boot Manager → Configurações de Inicialização Diversas**.
2. Use as teclas de seta para selecionar a **Política de OpROM de Armazenamento**.
3. Pressione **+** para alterar o valor para `UEFI Only`.

4. Pressione **F10** para salvar a alteração.

Para obter mais informações, consulte a documentação do ThinkServer.

Problemas de implantação do VMware ESXi

Use estas informações para solucionar problemas que você possa encontrar ao tentar implantar sistemas operacionais VMware ESXi em servidores gerenciados no Lenovo XClarity Administrator.

A implantação do VMware trava ou reinicia o sistema

Durante a instalação do VMware, 5.1u2 5.1u1, 5.1u3 ou 5.5 (qualquer atualização) em um servidor gerenciado, o servidor pode travar ou reiniciar.

Ele pode travar ou reiniciar logo após a seguinte mensagem:
```
Loading image.pld
```

O VMware 5.5 requer espaço de E/S mapeada em memória (MMIO) para ser configurado com os 4 GB iniciais do servidor. Dependendo da configuração, determinados servidores tentam usar uma memória maior que 4 GB, o que pode causar uma falha.

Conclua as etapas a seguir para resolver o problema:

Dica: Em vez de definir **MM Config** usando o Setup Utility de cada servidor, avalie a possibilidade de usar um dos padrões de UEFI estendida predefinidos relacionados à virtualização, o que configura a opção MM Config para 3 GB e desabilita a alocação do PCI 64-Bit Resource. Para obter mais informações sobre esses padrões, consulte Definindo configurações UEFI estendidas na documentação online do XClarity Administrator.

1. Reinicie o sistema. Quando `Press <F1> Setup` for exibido, pressione F1.
2. Selecione **System Settings → Devices and I/O Ports**.
3. Alterar a configuração de **MM Config** de 2 GB para 3 GB.
4. Assegure-se de que a configuração de **PCI 64-Bit Resource** seja definida como Disable.
5. Tente instalar a imagem do VMware novamente.

Falha de implantação do VMware com erros de disco

Durante a instalação do VMware ESXi, um erro relacionado à unidade de disco pode ser retornado e a implantação talvez não seja bem-sucedida.

A mensagem de erro pode ser semelhante ao seguinte exemplo:
```
error:/tmp/partitioning:line 2: install requires --disk
or --firstdisk
error:/tmp/partitioning:line 1: clearpart requires
one of the following arguments: --alldrives, --firstdisk,
--ignoredrives=, --drives=
```

Esse erro poderá ocorrer se o instalador do ESXi não detectar uma configuração SAS que esteja disponível para formatação e instalação. Normalmente, isso significa que a configuração do RAID no servidor está inativa ou configurada incorretamente. Como alternativa, isso poderá acontecer se um padrão de servidor tiver sido implantado com o Lenovo XClarity Administrator e **Desabilitar disco local** tiver sido selecionado para o padrão.

Conclua as etapas a seguir para resolver o problema:

- Se um padrão de servidor tiver sido implantado neste servidor e **Desabilitar disco local** estiver selecionado, atualize o padrão de servidor e implante-o novamente. Para obter mais informações sobre a configuração de armazenamento local usando padrões de servidor, consulte Definindo o armazenamento local na documentação online do XClarity Administrator.
- Valide se a configuração do RAID está correta no servidor:
  1. Reinicie o servidor e tente inicializar em uma opção legada pressionando F12 (escolha algo como HD0).
  2. Durante a inicialização, quando você vir informações sobre o adaptador SAS LSI, pressione Ctrl-C para alterar a configuração.
  3. Quando a interface do usuário for exibida, selecione **Propriedades do RAID** e **Exibir Configuração Existente**.
     - Se **Exibir Configuração Existente** não aparecer, isso indica que o RAID não foi configurado.
     - Se a configuração existente mostrar um status "Inativo", verifique se o RAID está configurado corretamente.

O sistema operacional não é reinicializado para concluir a implantação do ESXi em um servidor ThinkServer

Use essas informações para solucionar problemas que você poderá encontrar quando tentar implantar sistemas operacionais VMware ESXi em servidores gerenciados a partir do Lenovo XClarity Administrator quando o PXE está habilitado em uma placa de rede ou um dispositivo inicializável diferente da unidade de instalação estiver incluído na lista de ordem de inicialização.

Ao implantar o ESXi em um servidor ThinkServer, o sistema operacional não move explicitamente a unidade na qual o sistema operacional está instalado para a parte superior da lista de ordem de inicialização. Se um dispositivo de inicialização que contém um SO inicializável ou um servidor PXE for especificado antes do dispositivo de inicialização que contém o ESXi, o ESXi não será inicializado. Para a implantação do ESXi, o XClarity Administrator atualiza a lista de ordem de inicialização para a maioria dos servidores, para garantir que o dispositivo de inicialização ESXi esteja na parte superior dessa lista. No entanto, os servidores ThinkServer não fornecem uma maneira para o XClarity Administrator atualizar a lista de ordem de inicialização.

Se o servidor ThinkServer tiver adaptadores de rede que são inicializáveis em PXE, desabilite o suporte para PXE nesses adaptadores de rede, reimplante o sistema operacional e reabilite o suporte para PXE. Pressione F12 para interceptar a inicialização e acessar as configurações PXE. Para obter informações sobre como alterar as configurações de inicialização PXE, consulte a documentação do seu adaptador de rede.

Se o servidor ThinkServer tiver dispositivos inicializáveis na lista de ordem de inicialização além da unidade na qual o sistema operacional está instalado, remova-os dessa lista, reimplante o sistema operacional e depois volte a adicionar o dispositivo inicializável na lista. Certifique-se de que a unidade instalada esteja no topo da lista. Para obter informações sobre como alterar a lista de ordem de inicialização, consulte a documentação do ThinkServer.

Problemas de implantação do Red Hat e do SUSE Linux

Use estas informações para solucionar problemas que você possa encontrar ao tentar implantar sistemas operacionais Red Hat e SUSE Linux em servidores gerenciados no Lenovo XClarity Administrator.

O Redhat 6.x não pode ser implantado em servidor baseado em rack com IP estático

Poderá ocorrer um problema ao tentar implantar o Redhat 6.x em um servidor gerenciado se esse servidor estiver conectado da um comutador top-of-rack (TOR). Se o comutador TOR tiver o **protocolo de estrutura estendida** habilitado e o **encaminhamento por padrão** desabilitado, a imagem do Redhat talvez não seja baixada para o servidor.

Conclua as etapas a seguir para resolver o problema:

- Certifique-se de que o servidor esteja configurado para usar DHCP (e não um endereço IP estático). Em seguida, tente implantar o sistema operacional novamente.
- Modifique a configuração no comutador top-of-rack (TOR) para desabilitar o protocolo de estrutura estendida *ou* habilitar o encaminhamento de pacotes por padrão.

Falha na implantação do SO devido a drivers ausentes

Ao implantar o Red Hat® Enterprise Linux (RHEL) Server ou SUSE® Linux Enterprise Server (SLES) para um servidor, você pode ver uma mensagem de erro que interrompe a implantação, e o trabalho de implantação, por fim, expira.

Esse problema pode ocorrer quando a imagem do sistema operacional não contém drivers para dar suporte a todos os adaptadores que estão instalados no servidor gerenciado.

Os drivers não incluídos não são carregados em Lenovo XClarity Administrator para determinados adaptadores Mellanox IB. Portanto, a implantação de RHEL ou SLES em um servidor com esses adaptadores Mellanox não é permitida. Para obter mais informações sobre limitações do adaptador Mellanox, consulte o Página da Web Suporte do Lenovo XClarity Administrator para adaptadores Mellanox.

Problemas de implantação do Microsoft Windows

Use estas informações para solucionar problemas que você possa encontrar ao tentar implantar o Microsoft Windows em servidores gerenciados no Lenovo XClarity Administrator.

A implementação do SO falha devido a partições do sistema existentes em uma unidade de disco conectada

Ao implementar o Microsoft Windows em um servidor, as unidades de disco conectadas não devem ter partições do sistema existentes. Se uma partição for detectado, a implantação do SO falhará.

Execute uma das seguintes etapas para resolver esse problema.

- Desconecte a unidade de disco conectada.
- Exclua manualmente a partição do sistema na unidade de disco conectada.

  Atenção: A exclusão de partições em uma unidade de disco pode resultar na perda de dados. Certifique-se de fazer fazer backup de todos os dados na unidade de disco antes excluir partições.

  1. Em um prompt de comandos do Windows, execute o utilitário`diskpart` (consulte Site DiskPart Commands).
  2. Selecione o disco inserindo `select disk` <*number*>, em que <*number*> é o número do disco que contém a partição que você deseja excluir (consulte Site Selecione o disco).
  3. Selecione a partição a ser excluída, inserindo `select partition` <*number*> em que <*number*> é o número da partição no disco selecionado (consulte Site Selecione a partição).

4. Exclua a partição inserindo `delete partition override`. Os números de disco e partição são incluídos em mensagem de erro WinPE que aparecem quando uma partição de sistema é detectada e no log de trabalho. (consulte Site Exclua a partição

Capítulo 18. Problemas de controle remoto

Use esta informação para resolver problemas que podem ocorrer ao usar o aplicativo do controle remoto em Lenovo XClarity Administrator.

A sessão de controle remoto não inicia

Usa essas informações você tenta iniciar a sessão de controle remoto a partir da interface da web do Lenovo XClarity Administrator ou do atalho em seu sistema, mas ele não é iniciado.

Para resolver o problema, conclua as etapas a seguir.

1. Certifique-se que o servidor que você está conectando seja gerenciado por XClarity Administrator e que seu estado seja "Online" ou "Normal". Para obter mais informações sobre o status do servidor, consulte Visualizando o status de um servidor gerenciado na documentação online do XClarity Administrator.
2. Certifique-se de que as caixas de diálogo de pop-ups não estejam desabilitadas em seu navegador da Web para a sessão.
3. Certifique-se de que o navegador da Web tenha aceitado os certificados de segurança do XClarity Administrator. Geralmente, você será solicitado a aceitar o certificado na primeira vez que acessar o XClarity Administrator a partir de seu navegador.
4. Na janela Controle Remoto, clique em **Preferências → Geral → Sincronizar com servidor de gerenciamento** e aguarde um minuto. Em seguida, abra a sessão de controle remoto novamente.
5. Certifique-se de estar usando o JRE suportado para iniciar o aplicativo.
   - No Internet Explorer, clique em **Ferramentas → Opções da Internet → Avançado**. Certifique-se de que o JRE correto esteja selecionado (JRE versão 7.0, atualização 18 ou posterior).
   - No Firefox, clique em **Ferramentas → Opções → Aplicativos**. Certifique-se de que o Java Web Start Launcher esteja associado ao tipo de conteúdo JNLP.

   Nota: Garanta que a opção **Usar o formato SSL 2.0 ClientHello** *não* esteja selecionada no Painel de Controle Java.

   Se você estiver iniciando o aplicativo a partir do atalho em seu desktop, certifique-se de que o seu sistema local tenha conectividade com o XClarity Administrator. O aplicativo valida seu ID de usuário no servidor de autenticação XClarity Administrator.
6. Limpe o cache do Java Web Start no sistema local. Para liberar o cache do Java Web Start no sistema que está executando um sistema operacional Windows, execute o comando `javaws -uninstall`. Isso pode ser feito a partir do Painel de Controle do Windows no menu do JAVA.
7. O controle remoto requer que uma chave Features on Demand para o ThinkServer System Manager Premium Upgrade esteja instalada nos servidores ThinkServer. Para obter mais informações sobre chaves FoD instaladas nos seus servidores, consulte Visualizando chaves do Feature on Demand na documentação online do XClarity Administrator.

A sessão de controle remoto trava após o login

Use estas informações para resolver o problema quando a sessão de controle remoto é interrompida após o login.

Se você não estiver usando um dos JREs suportados, a sessão de controle remoto poderá ser interrompida após o login. Se a sessão de controle remoto aparece que foi interrompida depois de você fazer login, certifique-se de estar usando um JRE suportado para iniciar o aplicativo:

© Copyright Lenovo 2015, 2025

- Oracle JRE versão 6.18 ou posterior

Não é possível conectar-se a um servidor

Use estas informações para resolver o problema quando você não pode estabelecer uma sessão de controle remoto com um servidor.

Conclua as seguintes etapas para resolver esse problema.

- Garanta que você tenha os privilégios **lxc-supervisor**, **lxc-admin**, **lxc-security-admin**, **lxc-fw-admin**, **lxc-os-admin**, **lxc-hw-admin**, **lxc-service-admin** ou **lxc-hw-manager**.
- Certifique-se de que o sistema local tenha conectividade de rede e possa se conectar ao Lenovo XClarity Administrator.
- Certifique-se de que o servidor gerenciado esteja sendo gerenciado por XClarity Administrator clicando em **Hardware → Servidores** na barra de menu do XClarity Administrator.
- Se um firewall estiver instalado em seu sistema local, certifique-se de que ele permita conexões com o endereço IP para o servidor gerenciado.
- Ping o endereço IP do servidor gerenciado para certificar-se que seu sistema local tem conectividade com o servidor gerenciado. Se você estiver tentando acessar um servidor gerenciado de um sistema local que tenha um endereço IP de uma rede externa, ele também deverá ter um endereço IP que possa ser acessado externamente.
- Certifique-se de que o tunelamento do XClarity Administrator não tenha sido desativado para que o XClarity Administrator possa canalizar as solicitações de controle remoto para o servidor gerenciado que é a rede endereçável apenas na rede de gerenciamento privada. O tunelamento fica ativado por padrão.É possível habilitar o tunelamento do XClarity Administrator na caixa de diálogo Preferências do suporte remoto na guia **Segurança**. Para obter mais informações, consulte Configurando preferências de controle remoto.

Não é possível se comunicar com um comutador Flex System após iniciar uma sessão de controle remoto

Use estas informações para resolver o problema quando o Lenovo XClarity Administrator parar de se comunicar com um comutador de rede Cisco Nexus B22 Fabric Extender após iniciar uma sessão de controle remoto.

Se o CMM estiver configurado para usar a detecção automática, verifique se a porta de rede do comutador de rede Cisco Nexus B22 Fabric Extender está configurada para usar o modo de negociação automática.

Não é possível conectar-se a um servidor no modo de usuário único

Use estas informações para resolver o problema quando não é possível conectar-se a um servidor no modo de usuário único.

Quando você se conecta a um servidor em modo de usuário único, apenas uma sessão de controle remoto pode ser estabelecida com o servidor por vez.

Conclua as etapas a seguir para resolver o problema.

1. Tente conectar-se ao servidor gerenciado no modo multiusuário (se permitido, com base nos requisitos de segurança).
2. Entre em contato com outros usuários para determinar se alguém mais já estabeleceu uma sessão de controle remoto com o servidor gerenciado. Se a resposta for sim, aguarde até que o usuário finalize a sessão de controle remoto com o servidor gerenciado.

3. Tente conectar-se com o servidor gerenciado no modo de usuário único novamente.

O Controle Remoto pode se conectar a um servidor, mas nenhum vídeo está disponível

Use estas informações para resolver o problema quando você está conectado a um servidor de uma sessão de controle remoto, mas a sessão exibe a mensagem `No video available`.

Certifique-se de que o servidor esteja ligado e que o sistema operacional esteja executando em uma resolução e taxa de atualização suportadas.

A tabela a seguir lista as resoluções e taxas de atualização suportadas.

Tabela 1. Resoluções e taxas de atualização suportadas

Resolução	Taxas de atualização
640 x 480	60, 72, 75 e 85 Hz
800 x 600	60, 72, 75 e 85 Hz
1024 x 768	60, 72, 75 e 85 Hz
1440 x 900	60 Hz
1280 x 1024	60 e 75 Hz
1680 x 1050	60 Hz
1600 x 1200	60 e 75 Hz

Um servidor não aparece na lista para incluir uma nova sessão

Use essa informação para resolver um problema quando um servidor não aparecer na lista para incluir uma nova sessão, ou não aparecer mais na área de miniatura.

Conclua as etapas a seguir para resolver o problema.

1. Certifique-se de que o servidor gerenciado esteja sendo gerenciado por Lenovo XClarity Administrator by clicking **Hardware → Servidores** na barra de menu do XClarity Administrator.
2. Sincronize o inventário clicando guia **Geral** no menu de Preferências do Controle Remoto e, em seguida, em **Sincronizar com servidor de gerenciamento**. Para obter mais informações sobre as preferências do controle remoto, consulte Configurando preferências de controle remoto na documentação online do XClarity Administrator.

O estado do servidor na sessão de controle remoto não corresponde ao estado no Lenovo XClarity Administrator

Use estas informações para solucionar problemas quando o estado de um servidor gerenciado em uma sessão de controle remoto não corresponde ao estado do servidor gerenciado em Lenovo XClarity Administrator.

Conclua as seguintes etapas para resolver esse problema.

1. Certifique-se de que o servidor gerenciado esteja sendo gerenciado por XClarity Administrator clicando em **Hardware → Servidores** na barra de menu do XClarity Administrator.
2. Sincronize o inventário clicando guia **Geral** no menu de Preferências do Controle Remoto e, em seguida, em **Sincronizar com servidor de gerenciamento**. Para obter mais informações sobre as

preferências do controle remoto, consulte Configurando preferências de controle remoto na documentação online do XClarity Administrator.

Uma unidade ou imagem não pode ser montada em um servidor

Use essas informações para solucionar problemas ao tentar montar uma unidade ou imagem usando mídia remota, mas a unidade ou imagem não puder ser montada.

Conclua as etapas a seguir para resolver o problema.

1. Pare e reinicie a sessão de controle remoto.
2. Configure o modo de depuração como "Full" para a sessão de controle remoto. É possível configurar o modo de depuração em Preferências, na página **Geral**. Ao configurar o modo de depuração como "Full", o sessão de controle remoto gera arquivos de log de diagnóstico. Para obter mais informações sobre o modo de depuração, Configurando preferências de controle remoto.
3. Entre em contato com Suporte da Lenovo e forneça os arquivos de log. Para obter mais informações sobre como enviar dados diagnósticos para o Suporte da Lenovo, consulte Trabalhando com serviço e suporte.

A opção de mídia de armazenamento não é mostrada na lista de dispositivos de mídia remota disponíveis para montagem

Use estas informações para solucionar problemas quando a opção de mídia de armazenamento não é mostrada na lista de dispositivos de mídia remota disponíveis para montagem.

Se um CD, DVD ou dispositivo USB não aparecer na lista de dispositivos de mídia remota disponíveis a serem montados em um servidor gerenciado, clique em **Reiniciar usando conta de Administrador** no painel de mídia remota para acessar mais dispositivos locais.

A operação de energia não pode ser executada

Use estas informações para resolver problemas ao tentar executar uma operação de energia em um servidor gerenciado em uma sessão de controle remoto e que não poderá ser executada.

Quando você tenta executar uma operação de energia em um servidor gerenciado a partir de uma sessão de controle remoto, é possível receber uma mensagem informando que a operação de energia falhou ou que a operação de energia não é aplicável ao estado atual do servidor gerenciado.

Conclua as etapas a seguir para resolver o problema:

1. Certifique-se de que o servidor esteja sendo gerenciado por Lenovo XClarity Administrator. Para obter mais informações, consulte Visualizando o status de um servidor gerenciado na documentação online do XClarity Administrator.
2. Na página Servidores, verifique se o status de servidor é válido.
3. Certifique-se de que a operação de energia é válida para o estado atual do servidor. Por exemplo, se o servidor está desligado atualmente, emitir um desligamento não funcionará.
4. Verifique o log dos trabalhos para ver se a operação de energia foi concluída. Pode levar um certo tempo para a operação ser concluída, dependendo do carregamento atual do XClarity Administrator. Para obter mais informações sobre como exibir o status do trabalho, consulte Monitorando trabalhos.

Vídeo indisponível ao conectar no Servidores Flex System x280 X6, x480 X6 e x880 X6

Use estas informações para resolver problemas ao tentar iniciar uma sessão de console remoto com um sistema de vários nós Servidores Flex System x280 X6, x480 X6 e x880 X6 ou quando nenhum vídeo aparece na nova guia.

Conclua as etapas a seguir para resolver o problema.

1. Termine conexão que você acabou de iniciar se ainda estiver ativa fechando uma nova guia.
2. Certifique-se de iniciar uma conexão remota com o servidor *primário* na configuração de vários nós.

Capítulo 19. Problemas da interface do usuário

Use estas informações para solucionar problemas de interface do usuário.

Itens de menu, ícones da barra de ferramentas e botões estão desativados (esmaecidos)

Use estas informações para solucionar problemas quando determinadas ações estiverem desativadas na interface do usuário.

Uma *função* é usada para controlar o acesso do usuário a recursos e limita as ações que os usuários podem executar nesses recursos. O *grupo de funções* é uma coleção de um ou mais funções e é usada para atribuir essas funções aos diversos usuários. As funções que você configura para um grupo de funções determinam o nível de acesso que é concedido a cada usuário que é um membro deste grupo de funções. Cada usuário do Lenovo XClarity Administrator deve ser membro de pelo menos um grupo de funções. Para obter informações sobre funções e privilégios, consulte Gerenciando funções na documentação online do XClarity Administrator.

Certifique-se de que sua conta de usuário esteja atribuída a um grupo de funções que tenha privilégios necessários para executar a ação. Para obter mais informações, contate o administrador do sistema.

Navegador da Web não responde quando várias guias estão abertas

Quando várias guias contendo páginas do Lenovo XClarity Administrator estão abertas, o navegador da Web pode travar ou ficar sem resposta

O XClarity Administrator usa JavaScripts do cliente que trocam uma grande quantidade de dados com o servidor de gerenciamento. Quando várias guias estão abertas, o navegador da Web consome mais de memória, ciclos de processador e largura de banda da rede. Várias guias podem fazer causar falha nos navegadores ou deixá-los sem resposta. O efeito varia de acordo com as versões e os tipos de navegador da Web.

Para resolver esse problema, reduza o número de guias do navegador da Web que contêm páginas do XClarity Administrator.

Para obter mais informações, consulte Dica HT504133

Falha na resposta de JSON, erro de análise e outros erros inesperados

Use estas informações para solucionar problemas de resposta do JSON.

Faça logout do Lenovo XClarity Administrator e tente repetir o login.

A interface do usuário não está no idioma preferencial

Use estas informações para solucionar problemas com preferências de idioma.

1. Certifique-se de que o navegador da Web esteja usando o código do seu idioma preferencial.
2. Na barra de título do Lenovo XClarity Administrator, clique no menu de ações do usuário (

) e clique em **Alterar idioma**. Selecione o idioma que você deseja exibir e, em seguida, clique em **Fechar**.

© Copyright Lenovo 2015, 2025

Tempos de carregamento lentos ou aparentemente sem resposta, longa espera para atualizar, renderização incorreta

Use estas informações para solucionar problemas com a interface do usuário.

1. Atualize a página com o botão **Atualizar** do seu navegador da Web.
2. Limpe o cache do navegador da Web e recarregue a página.

Perda de dados inesperada

Use estas informações para solucionar problemas da perda de dados no Lenovo XClarity Administrator.

Se o sistema operacional do host tiver sido desligado inesperadamente, restaure o XClarity Administrator do backup mais recente (consulte Fazendo backup e restaurando o XClarity Administrator na documentação online do XClarity Administrator).

As alterações de local do dispositivo não são refletidas na exibição de rack

Use estas informações para solucionar problemas da exibição de rack em Lenovo XClarity Administrator.

Se você alterar o local de um dispositivo usando um das APIs REST a seguir ou usando o Baseboard Management Controller após o dispositivo ser gerenciado pelo XClarity Administrator, as alterações não serão refletidas na exibição de rack na interface do usuário do XClarity Administrator. Edite as propriedades do dispositivo ou o rack na interface do usuário para refletir as alterações feitas na API ou no controlador de gerenciamento (consulte Alterando as propriedades do sistema para um servidor, Visualizando os detalhes de um chassi gerenciado e Gerenciando racks na documentação online do XClarity Administrator).

- PUT /canisters/<*UUID*>
- PUT /chassis/<*UUID*>
- PUT /nodes/<*UUID*>